Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Ekonomický a environmentální dopad těžby kryptoměn

Matěj Beránek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Matěj Beránek

Podnikání a administrativa

Název práce

Ekonomický a environmentální dopad těžby kryptoměn

Název anglicky

Economic and environmental impact of cryptocurrency mining

Cíle práce

Cílem práce je zjistit a změřit, jaký dopad má těžba kryptoměn na životní prostředí. Dílčím cílem je zjistit ekonomickou výhodnost těžby kryptoměn.

Metodika

Teoretická část bakalářské práce bude založena na studiu a analýze odborných informačních zdrojů.

Teoretická část bude zaměřena na fakta o ekonomickém a enviromentálním dopadu těžby kryptoměn a používání počítačů. Dále bude prezentována teorie využitelná v praktické části.

V praktické části bude měřena průměrná spotřeba energie počítače bez spuštěných aplikací a ta bude porovnána se spotřebou energie počítače, který bude mít spuštěnou těžící aplikaci. Budou porovnány 3 těžící aplikace v tom, kolik energie bude na těžbu kryptoměny vynaloženo a kolik bude, při v tu dobu aktuálním kurzu kryptoměny, vyděláno.

Výsledky budou prezentovány formou tabulek a grafů.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

kryptoměna, počítače, životní prostředí, ekonomický dopad

Doporučené zdroje informací

Bitcoin a jiné kryptopeníze budoucnosti, Dominik Stroukal; Jan Skalický, ISBN: 978-80-271-1043-8
Bitcoin: Peníze budoucnosti, Jan Skalický, Dominik Stroukal, ISBN: 978-80-877-3328-8
Cryptocurrency Mining For Dummies (anglicky), Peter Kent, Tyler Bain, ISBN: 978-11-195-7929-8
Jak pochopit Bitcoin, Michael Merta, ISBN: 999-00-030-7519-2

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Ivana Hellerová

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 13. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci „Ekonomický a environmentální dopad těžby kryptoměn" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval Ing. Ivaně Hellerové za vedení mé bakalářské práce.

Ekonomický a environmentální dopad těžby kryptoměn

Abstrakt

V teoretické části práce je pojednáváno o kryptoměnách obecně, co si pod tím pojmem má člověk představit. Dále je popsána architektura nezbytné technologie pro funkci kryptoměn, její historie a vývoj dalších historicky významných kryptoměn. Následně je popsán hlavní představitel kryptoměn, Bitcoin, o kterém je pojednáváno dopodrobna. Je pohlíženo na těžbu Bitcoinu, kterou se zabývá praktická část práce, a na jeho ekonomické hledisko.

V praktické části je popsána metodika využitá k dosažení výsledků prezentovaných na konci této práce. Poté jsou popsány některé důležité koncepty týkající se těžby, které autor zohlednil v rozhodování při výběru těžební aplikace a následně i těžebních bazénů a dalších služeb, které jsou využity k objektivnímu zobrazení výsledků těžby. Výtěžky a hodnoty naměřené v průběhu těžby jsou zpracovány do přehledných a vypovídajících grafů, porovnány s klidovými teplotními hodnotami a hodnotami spotřeby pro vyhodnocení ekologického dopadu v malém měřítku. Pro demonstraci ekologického dopadu ve velkém měřítku je čerpáno z externích zdrojů a porovnáváno s hodnotami celých států.

Klíčová slova: kryptoměna, počítače, životní prostředí, ekonomický dopad, těžba, rentabilita, těžební software

Economic and environmental impact of cryptocurrency mining

Abstract

The theoretical part of the thesis deals with cryptocurrencies in general, what one should imagine under this term. Furthermore, the architecture of the necessary technology for the function of cryptocurrencies, its history and the history of significant cryptocurrencies are described. Subsequently, the main representative of cryptocurrencies, Bitcoin, is described in detail. The mining of Bitcoin, which is dealt with in the practical part of the thesis, and its economic aspect are looked at.

The practical part describes the methodology used to achieve the results presented at the end of this thesis. Then, some important concepts related to mining were described, which are taken into account in the decision making process for the selection of the mining application and subsequently the mining pools and other services that were used to objectively display the mining results. Yields and values measured during the process are compiled into clear and telling graphs, compared with resting temperature and consumption values to evaluate the ecological impact on a small scale. To demonstrate ecological impact on a large scale, external sources were drawn upon and compared with particular national values.

Keywords: cryptocurrency, computers, environment, economical impact, mining, rentability, mining software

Obsah

1 Úvod

Životní prostředí je v současnosti velmi diskutované téma a lidé a technologický vývoj na něj mají stále větší vliv. Rychlý vývoj výpočetní techniky spolu s kryptografií a potřebou anonymity daly vzniknout dnešním kryptoměnám. O Bitcoinu, největším zastupiteli kryptoměn, slyšel skoro každý, ovšem jen málo lidí ví, jaký dopad má na životní prostředí. Tato práce se zabývá dopady těžby kryptoměn na životní prostředí a otázkou, zdali se v dnešní době vůbec vyplatí běžnému člověku kryptoměny těžit.

Teoretická část práce je založena na poznatcích získaných z odborných publikací, článků a internetových zdrojů. Věnuje se tématu kryptoměn, jejich historii, Blockchainu a jeho historii a největšímu představiteli kryptoměn - Bitcoinu. Bitcoin je popsán z hlediska tradiční ekonomie. Jsou popsána obecně známá fakta a důležité milníky vývoje a je popsán i proces jeho těžby a vše nutné k pochopení tohoto procesu.

První blok praktické části je dedikován metodice následující práce, informacím nutným k provedení informovaného výběru vhodného těžebního softwaru a samotnému výběru. Jsou popsány jednotlivé metody těžby kryptoměn a první blok je ukončen jejich porovnáním. Dále jsou vysvětleny těžební bazény, naprosto nezbytný koncept pro získání jakéhokoli zlomku jakékoli kryptoměny. Bez nich by byla konkurence příliš velká na to, aby člověk sám vytěžil nějaké množství kryptoměny.

V druhém bloku je popsána provedená těžba samotná, jsou měřeny a sledovány stanovené hodnoty a následně vyhodnoceny a zpracovány do grafů.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je zjistit a změřit, jaký dopad má těžba kryptoměn na životní prostředí. Dílčím cílem je zjistit ekonomickou výhodnost těžby kryptoměn.

2.2 Metodika

Teoretická část bakalářské práce je založena na studiu a analýze odborných informačních zdrojů.

Teoretická část je zaměřena na fakta o ekonomickém a enviromentálním dopadu těžby kryptoměn a používání počítačů. Dále je prezentována teorie využitelná v praktické části.

V praktické části je měřena průměrná spotřeba energie počítače bez spuštěných aplikací a ta je porovnána se spotřebou energie počítače, který měl spuštěnou těžící aplikaci. Kromě spotřeby elektřiny je měřena i teplota grafické karty počítače v průběhu těžby a tyto hodnoty jsou porovnány s klidovou hodnotou. Jsou porovnány 3 těžící aplikace z hlediska toho, kolik energie bylo na těžbu kryptoměny vynaloženo a kolik bylo, při v tu dobu aktuálním kurzu kryptoměny, vyděláno. Rentabilita je posouzena napříč časem, kde jsou 2 proměnné: velikost odměny za vytěžení bloku Bitcoinu a průměrná cena elektřiny v České republice.

Výsledky jsou prezentovány formou tabulek a grafů.

3 Teoretická východiska

3.1 Kryptoměny

Kryptoměny mají mnoho zástupců, můžeme se na pojem dívat jako na systém nebo jednotlivé zástupce.

Zástupce kryptoměny si můžeme představit stejně jako české koruny, euro či americký dolar, stejně jako tyto vyjmenované měny, jsou ukládány v peněženkách. Kryptoměna je nositelem nějaké finanční hodnoty. Rozdílů mezi jmenovanými měnami a obecnou kryptoměnou je mnoho. Prvním je ten, že kryptoměny nemají fyzickou podobu, jsou čistě digitální či virtuální. Druhým rozdílem je systém, který kryptoměny používají. Kryptoměny používají decentralizovaný systém, ve kterém není žádná autorita, která má možnost regulace trhu, na rozdíl od „reálných peněz“, které jsou vydávány a spravovány centralizovaným systémem, bankou. Každá z kryptoměn používá ke svému chodu a zápisu každé transakce šifrovací algoritmus. (1)

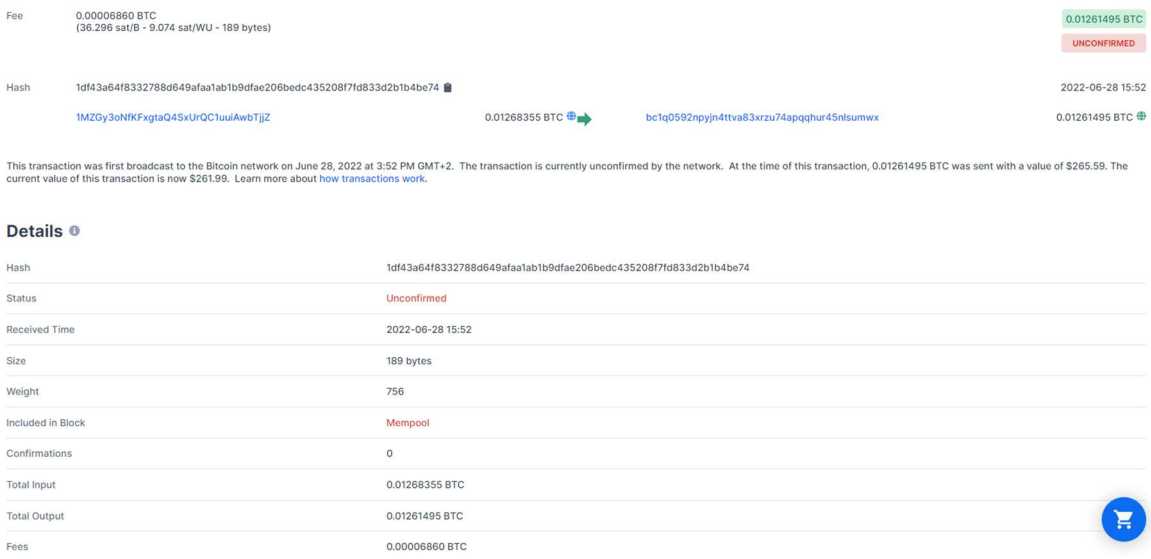
Kryptoměnu si můžeme představit jako systém digitálních plateb, podobný internetovým bankovnictvím, s tím rozdílem, že nespoléhá na banky. Každému uživateli kdekoliv na světě umožňuje odesílat a přijímat peníze. Tento systém však na rozdíl od měn ve skutečném světe používá adresy, které k dané reálné identitě ve světě nemusí být nijak připojeny. (1)

3.2 BlockChain

BlockChain v překladu znamená řetězec bloků. V praxi to znamená, že se na sebe jednotlivé bloky odkazují. Odkazují se na sebe od konce k začátku, druhý na první, třetí na druhý atd. Odkazují se na sebe prostřednictvím tzv. hashe (dlouhý řetězec zašifrovaných informací). Každý blok má tak svého unikátního předka a odkazuje se na něj adresou jeho hashe. Výjimkou je první (genesis block), který namísto informace hashe předka má vepsanou nulu.

Každý z bloků v sobě uchovává informace o předchozích blocích a provedených transakcích, čímž jsou považovány za validní. Tímto způsobem odkazování se jednoho bloku na předešlý je historie BlockChainu nepřepsatelná, jelikož kdyby někdo chtěl přepsat jakýkoli blok, musel by přepočítat veškeré jeho následující bloky (bloky, které obsahují hash přepisovaného bloku nebo odkaz na tento hash). Toto složité přepočítání všech následujících bloků je způsobeno avalanche effectem (vysvětleno níže). (2)

Valná většina kryptoměn a jejich hlavní představitelé, kterými jsou například Bitcoin, Ethereum, DogeCoin, Cardano a mnohé další, běží na systému jménem BlockChain. BlockChain si můžeme představit jako operační systém, jako každý jiný, avšak tento operační systém je specializován na záznam veškerých typů transakcí. Síť BlockChain má strukturu Peer-to-Peer (P2P) sítě, což znamená, že jednotliví uživatelé BlockChainu (počítače) se zároveň stávají informačními uzly v dané síti. Využití sítě P2P má oproti běžné centralizované síti mnoho výhod. Pokud si jako příklad vezmeme banku, banka má hlavní (centrální) server, na kterém uschovává veškerá data, což znamená, že pokud se někomu podaří prolomit ochranu daného serveru, veškerá data dané banky jsou v ohrožení, stejně jako peníze klientů dané banky. Výhoda využití P2P sítě tkví v tom, že každý jeden uživatel (tzv. uzel sítě) se zároveň stává i uchovatelem malé části informací o celé síti. Tato data jsou rozprostřena mezi veškeré uzly sítě zároveň, což znamená, že pokud by někdo chtěl napadnout BlockChain, nebo kteroukoliv kryptoměnu, která na BlockChainu běží, musel by napadnout veškeré uzly dané sítě, což je prakticky nemožné. Díky tomuto se nemůže stát, že by byla jedna specifická, nebo jakýkoliv počet transakcí přepsán. V každý moment je více počítačů, které drží informace o dané transakci a při pokusu o přepsání informací o této transakci v síti, mezi sebou dané uzly porovnají uchované informace a případnou změnu zamítnou. Každá transakce v síti BlockChain je viditelná v reálném čase a je o ní vše dohledatelné. Je vidět, ze které „peněženky“ (adresa, na které se uchovávají kryptoměny) byla kryptoměna odeslána, ve prospěch které peněženky transakce proběhla, množství kryptoměny, je vidět i její hash (unikátní identifikátor transakce). BlockChain tedy slouží jako naprosto transparentní účetní kniha, která je bezpečnější než běžná centralizovaná síť, na kterou jsme dnes zvyklí. Největší výhodou této sítě je, že transakce probíhají okamžitě, nemají zprostředkovatele a poplatky jsou minimální. Dnes každý podnik má své vlastní účetnictví a mnohdy si najímají účetní agentury, které jejich účetnictví spravují. Proto má BlockChain nevyužitý potenciál. (3)



Obrázek 1 - Detaily náhodné transakce v BlockChain (4)

Dostupnost:
https://www.BlockChain.com/btc/tx/1df43a64f8332788d649afaa1ab1b9dfae206bedc435208f7fd833d2b1b4be74

3.2.1 Mechanismy BlockChainu

PoW (Proof-of-Work) je decentralizovaný mechanismus, který funguje na shodě uživatelů sítě a na shodnosti dat. Každý uživatel sítě (bavíme se zde o počítači) musí průběžně vypočítávat libovolné matematické úkoly, čímž se zabraňuje tomu, aby někdo zneužil nebo okrádal systém. Mechanismus PoW je běžně využíván napříč mnohými kryptoměnami, ať už se jedná o samotnou těžbu nebo verifikaci transakcí. Díky tomuto není v systémech kryptoměn potřeba existence nějaké centralizované autority, která by musela každou transakci ověřovat a potvrzovat, jelikož takto si je systém sám schopen ověřit validitu probíhajících plateb. Společným fungováním BlockChainu a PoW je prakticky nemožné si „připsat“ Bitcoin, nebo kteroukoli jinou kryptoměnu, která na BlockChainu funguje. Způsob, kterým jednotlivé uzly v síti poznají, že se někdo snaží upravit informaci v systému, je pomocí hashe. Hash je dlouhý řetězech čísel, které slouží jako důkaz práce. Vezmeme-li v úvahu specifické informace zadané do systému, vždy vygenerují jen jeden, informacím odpovídající, hash. V hashovacích systémech je něco, čemu se říká „avalanche effect“ (lavinový efekt), který způsobuje, že malá jednoduchá změna v datech vygeneruje diametrálně odlišný hash. Hashování je jednostranná funkce kontroly, není možné ji použít k získání původních dat, pouze ke kontrole, zda data vygenerovaná hashem odpovídají původním datům. O hashování je pojednáno v kapitole o těžbě Bitcoinu. (5) (6)

Je jedna věc, které se BlockChainu daří předcházet, a to je Double Spend (dvojí útrata). Není tomu zamezeno jakýmsi mechanismem, avšak samotnou architekturou BlockChainu. Double Spend byl důvod pádu nejedné kryptoměny před Bitcoinem a využívá to decentralizovaného systému. Double Spend je koncept, který zneužívá toho, že kryptoměny jsou „pouhou“ digitální informací a snaží se stejné jednotky kryptoměny využít k uhrazení více plateb. Toto by bylo možné, kdyby příjemce platby nevyžadoval potvrzení o dané platbě. Čím méně potvrzení adresát transakce požaduje, tím snazší útok je. Útočník je v každém případě nucen vytěžit dané bloky, čemuž musí obětovat svůj výpočetní výkon. Nejistota tohoto útoku roste s rostoucím počtem vyžadovaných potvrzení. Tím, že potvrzení je vyžadováno od celé sítě BlockChainu, tak je tomuto typu útoku zamezeno. Double Spend využívá decentralizovaného systému, ovšem užití centralizovaného systému by nebyla prevence. Pokud by někdo dostatečně šikovný byl schopen centrální autoritu zničit (hackerským útokem), útok bude proveditelný. (2)

3.2.2 Historie BlockChainu

BlockChain a jeho vznik je stejně jako vznik Bitcoinu připisován Satoshi Nakamotovi. Bitcoin je bez pochyby výtvorem autora Nakamota, avšak vznik BlockChainu je složité připsat jednomu autorovi. První zmínka o BlockChainu, byla v akademické disertaci „Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups“ autora Davida Chauma v roce 1982. David Chaum položil základy BlockChainu, jeho architekturu, generace před vznikem Bitcoinu. BlockChain nebyl specificky navržen pro podporu kryptoměn, ale zakladatel technologie v technologii samotné shledal potenciál k tomuto využití. V roce 1989 založil společnost DigiCash, která roku 1995 představila první kryptoměnu digicash (také eCash nebo cyberbucks). Kryptoměna digicash slibovala vlastnosti mnohých moderních kryptoměn. Hlavním marketingovým bodem Chaumovy kryptoměny byla anonymita. David vytvořil šifrování na takové úrovni, že ani vláda údajně nebyla schopna dešifrovat, kdo komu kolik poslal. Společnosti DigiCash se však nepodařilo přesvědčit banky, aby se k projektu připojily. V té době nebyla dostatečná internetová infrastruktura, tudíž jeho model BlockChainu založený na P2P (peer to peer) síti nemohl fungovat. David Chaum nejspíše předběhl svou dobu a měl nadčasové nápady, dříve, než na ně byl svět připraven a tak jeho firma DigiCash roku 1998 vyhlásila bankrot. Historie BlockChainu se opět stala zajímavou roku 2008, kdy vyšel

výzkumný článek „Bitcoin: A Peer-to-Peer Electronic Cash System“ pod jménem autora Satoshi Nakamoto. Dle expertů je protokol BlockChain popsaný ve vědecké práci Nakamota v podstatě stejný jako ten od Davida Chauma, akorát rozšířený. (7) (8)

Nakamoto tento protokol rozšířil o dnes velice běžně užívaný mechanismus PoW (Proof-of-Work). Tento systém byl roku 2004 upraven Halem Finneym k využití pro zabezpečení kryptoměn skrze myšlenku „reusable proof of work“ (opakovatelně použitelného důkazu práce) pomocí algoritmu SHA-256. Tento koncept byl představen v roce 2009 a krátce poté se Bitcoin stal první aplikací Finneyho myšlenky. Finney byl prvním příjemcem Bitcoinové transakce. (7)

Satoshi Nakamoto je jistě pouhý pseudonym pro autora nebo skupinu autorů. Jelikož na jeho blogu byla vždy použita perfektní angličtina. Avšak byly zaznamenány i chybné pokusy o použití dobového amerického slangu. To napovídá, že autor je z anglicky mluvící země. (2)

3.2.3 Historie dalších důležitých kryptoměn

Kryptoměny se při mnohých pokusech o jejich založení potýkaly s mnohými problémy. Hlavním problémem bylo, že pokusy o založení nové měny byly vnímány autoritami jako potenciální konkurence státních peněz. První významnou kryptoměnou byla Chaumův eCash. Chaum nikdy nesouhlasil se státním zřízením a představením eCash chtěl uživatelům poskytnout anonymitu, což mohlo být jedním z důvodů, proč se mu nedostalo státních peněz k uvedení eCash do praxe. Netrvalo to však dlouho, než se na povrchu objevily další, dnešnímu Bitcoinu podobné, kryptoměny. Mezi ně patřily e-gold, 1mdc, liberty dollar, liberty reserve, e-bullion a další.

Mnohé kryptoměny byly založeny na ideji zlatého standardu monetárního systému, kdy měly peníze dle Aristotelovy definice „vnitřní hodnotu“. Vnitřní hodnota peněz spočívá v tom, že kdyby se celý monetární systém zhroutil a peníze pozbyly své hodnoty, je ještě jiný způsob, jak jich využít. V době zlatého standardu byly peníze kryté zlatem, což znamenalo, že i kdyby peníze ztratily svou hodnotu, bylo by stále možné je směnit za odpovídající množství zlata. (2)

3.3 Bitcoin

3.3.1 Bitcoin a tradiční ekonomie

Aristoteles měl několik kritérií, které musely být splněny, aby měna byla považována za „dobré peníze“.

- Dělitelnost
- Skladovatelnost a přenositelnost
- Zaměnitelnost
- Vnitřní hodnota

Dělitelnost je u kryptoměn na daleko nejvyšší úrovni. Obzvlášť tím, že jeden Bitcoin má tak vysokou hodnotu. Je třeba mít jednotky, které jsou miniaturními zlomky jednoho Bitcoinu, aby se dala uhradit zcela přesná hodnota. Stejně jako česká koruna má centrální autoritou (ČNB) stanovené bankovky a mince, které všichni známe, i Bitcoin má své stanovené a pojmenované hodnoty (zlomky). Hodnota jednoho Bitcoinu (pokud se bavíme o jednotce kryptoměny, je nutno ji označovat s malým „b“ a její zkratka je BTC) je příliš vysoká pro běžné platby, tudíž má odvozené jednotky. Pokud je použito slovo Bitcoin s velkým „B“ je tím míněna kryptoměna obecně. CentiBitcoin (cBTC = 0,01 BTC), miliBitcoin (mBTC = 0,001 BTC), mikroBitcoin (μBTC = 0,000001 BTC) a nejmenší jednotkou je ‚satoshi‘ (1 satoshi = 0,00000001 BTC = $1,0 \times 10^{-8}$), která je tak pojmenována na počest zakladatele Bitcoinu Satoshiho Nakamota. V porovnání s historicky uznanými měnami, ať už je to cenný kov, nebo dnešní tradiční peníze, Bitcoin je mnohem snáz dělitelný na menší zlomky, než kterákoli jiná měna. První kritérium je splněno. (2)

Skladovatelnost a přenositelnost: Aristoteles tvrdí, že podmínkou pro dobré peníze je jejich snadné skladování a přenášení. Skladovatelnost u drahých kovů nebyla takovým problémem, jako přenositelnost. Poslat zlatou cihlu na druhý konec světa nebyla běžná praktika. Dnešní peníze ani s jednou vlastností nemají problém. Peníze uložíme do banky, na spořící účty a během pár kliknutí a pár sekund mohou být na druhém konci světa. Na Bitcoin se lze dívat jako na digitální informaci, což nám dává možnost širokého výběru jeho skladování. Můžeme použít hardwarové peněženky, softwarové peněženky třetích stran, harddisk nebo telefon. Co se přenositelnosti týče, jako digitální informaci je stejně snadné ho odeslat jako peníze z účtu, stačí vědět kam, kolik a po pár kliknutích je Bitcoin na druhé straně světa. Druhé kritérium je splněno. (2)

Zaměnitelnost se vztahuje na specifickou jednotku peněz nebo něčeho, co nějakou hodnotu drží. Ideální případ pro vysvětlení jsou bankovky. Pokud kamarádovi půjčíme 500 Kč

bankovku a druhý den nám ji vrátí, ale není to ta samá bankovka s tím samým sériovým číslem, ani o tom nevíme. Vyjadřuje to totožnou hodnotu jako zapůjčená bankovka, tak ani nekontrolujeme, zdali je to ta samá či nikoliv. U Bitcoinu je to stejné, je nám jedno jaký Bitcoin se nám dostane zpátky. (2)

Vnitřní hodnota je snad nejdůležitějším kritériem dobrých peněz vůbec. Aristoteles tím míní využitelnost i mimo monetární systém. Příklad na drahých kovech je následující: kdyby zlato přestalo být vyhledávané jako nositel hodnoty kvůli své vzácnosti, stejně by mělo jisté využití jako polovodič. Dnešní tradiční peníze jsou na tom obdobně, mince až tak ne, ale bankovky by se při nejhorším, kdyby monetární systém nefungoval a peníze ztratily svou hodnotu, daly využít i jiným způsobem. Přesně toto se stalo v poválečném Německu v důsledku hyperinflace v roce 1923, kdy Německo odstoupilo od zlatého standardu, vydávaly se nekryté bankovky a v průběhu války, za 4 roky narostlo množství peněz v oběhu na pětinásobek, a to byly ještě stanoveny úřední ceny surovin, potravin a dalších potřeb. Hyperinflace ovšem nastala až roku 1923, kdy Němci v červenci potřebovali 353 412 marek na koupi jednoho dolaru a pouze o měsíc později je jeden dolar vyšel na 4 620 455 říšských marek. V říjnu 1923 stál litr mléka 5,4 milionů marek. Jak nám historie napovídá, je možné, že v důsledku špatného rozhodování, státní měna ztratí veškerou svou hodnotu, takže Aristotelovo volání po vnitřní hodnotě je oprávněné. (2) (9)

Čím je tedy krytý Bitcoin? Existují mylné představy o tom, že Bitcoin je krytý energií spotřebovanou na těžbu, matematickým výkonem těžících soustav, matematikou či kryptografií samotnou, nebo dokonce samotnou prací Satoshiho Nakamota. Veškeré tyto domněnky jsou nesmyslné, protože jsou to všechno věci minulosti, od spotřebované energie přes samotný výpočet až po práci Satoshiho Nakamota. V tento moment by byl Aristotelem Bitcoin s největší pravděpodobností zavržen. Autor však tvrdí, že by se Aristoteles v tomto výroku mýlil. Jak se autor zmínil u zlata, je vzácné, protože ho není neomezené množství. Bylo by stejně tak drahé, kdybychom ho měli neomezenou zásobu? Podle autora ne, a to je to samé jako s Bitcoinem. Jak zjistíme v další kapitole, Bitcoin má omezené maximální množství bitcoinů. Tento element Bitcoinu přidává na hodnotě, jelikož je jako komodita vzácný. Ať se to týká sběratelství z jakéhokoli odvětví, zpravidla ty nejdražší kusy jsou drahé jen kvůli jejich omezenému počtu a neexistující možnosti získat další originální kus. Na příkladu sběratelství nejdražších aut na světě (Ferrari 250 Grand Turismo Omologato) je již pouhých 33 kusů a jeden z nich se v roce 2018 prodal za rekordní cenu $70 000 000 (v přepočtu na koruny v kurzu daného měsíce

1 545 180 000 Kč). Jakýkoliv předmět směny má svou hodnotu, která se odvíjí od možnosti užitku. Bitcoin má nemalé spektrum možností užitku, které se postupně zvětšuje. (10) (11) (2)

3.3.2 Bitcoin obecně

Bitcoin je bez pochyb nejznámější kryptoměnou na světě a pozornost začal vzbuzovat již v roce 2011. Celý svět byl zprvu skeptický, první myšlenka, která lidi napadala při slovech „virtuální měna“ byla, že to nebude ničím kryté. Taková měna už existovala, zlato. Zlato i papírové peníze měly však na rozdíl od virtuální měny nějaké využití. Zlato je drahý kov využitý v mnohých technologiích a penězi se přinejhorším dá zatopit. (2)

Bitcoin zaznamenal největší mediální pozornost v roce 2013, kdy jsme logo Bitcoinu mohli vidět ve zprávách, novinách a slyšet o něm v rádiu. Důvodem této pozornosti byl extrémní nárust ceny. (2)

Nejnižší cena byla zaznamenána v roce 2013 dne 5.7., kdy jeden Bitcoin stál 68,43$ a svou nejvyšší cenu toho roku zaznamenal dne 4.12., kdy se cena dostala na 1157,17$. Toto znamenalo nárust ceny o 1691 % během pěti měsíců. (12)

Tento cenový nárust pochopitelně zaujal mnohé ekonomy, investory, ovšem i odborníky z odvětví IT, kteří žasli nad jeho kódem. (2)

V minulé kapitole jsem představil BlockChain a jeho strukturu v podobě P2P sítě. Bitcoin má nastavené maximální množství Bitcoinů, které kdy bude existovat. Tento limit je také znám jako „hardcap“, který je v kódu samotného Bitcoinu a jednotlivých uzlech sítě. Limit Bitcoinu je nastaven na 21 milionů bitcoinů. V říjnu roku 2009 bylo do oběhu vypuštěno 1,3 z maximálních 21 milionů Bitcoinů (BTC). (13)

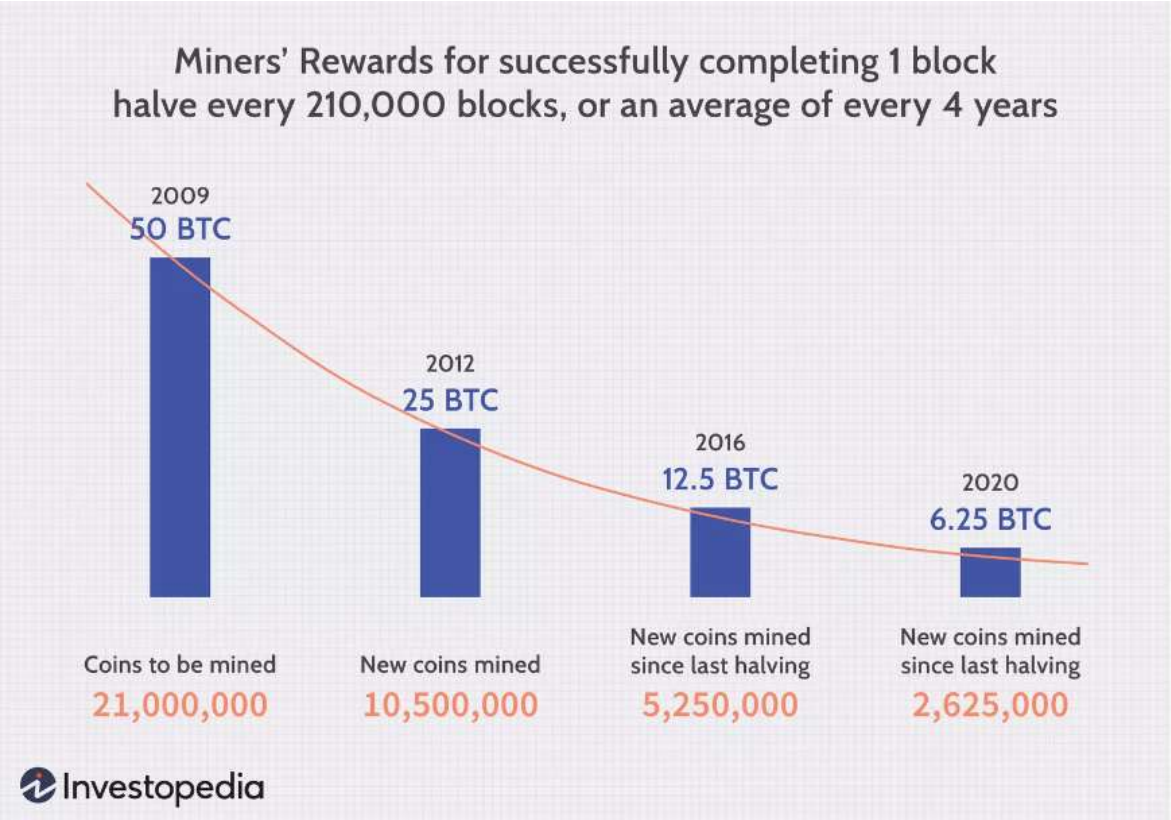
3.3.3 Těžba Bitcoinu

Pro vysvětlení „těžby“ Bitcoinu bude třeba znalostí o hashování z předchozí kapitoly. Pro dnešní počítače by bylo triviální vygenerovat libovolný hash. To je však regulováno sítí Bitcoinu. Síť zvolí „obtížnost“, aby se z vygenerování náhodného hash opravdu stala práce. Tato práce jednotlivých uzlů zajišťuje chod celé sítě. Toto nastavení je upraveno tak, aby mohl být „vytěžen“ nový blok – přidán do BlockChainu vygenerováním nového platného hashe. Toto se podaří přibližně jednou za každých 10 minut. Obtížnost je nastavena cílovou hodnotou pro hash. Čím nižší je cílová hodnota, tím menší je množina možných hashů a tím složitější je takový hash vygenerovat. V praxi to znamená hash, který začíná dlouhou sérií nul. V tomto bodě už má síť nastavené kritérium obtížnosti pro „těžaře“, avšak tu musí nějak zpracovat jednotlivé uzly. Do zadání si musí každý uzel vyplnit toto kritérium, které má číselnou podobu.

Tomuto číslu se říká „nonce“ (number only used once). Nonce je čtyř bitové číslo, přidané k hashovanému nebo zašifrovanému bloku v BlockChainu, které při opětovném hashování splňuje podmínku náročnosti zadanou Bitcoin sítí. Těžba je konkurenční proces, avšak svou povahou má blíž k loterii než k závodu. Jak autor již zmínil, vyhovující důkaz práce je v průměru vygenerován jednou za deset minut, kdo ho však vygeneruje je otázkou, na kterou nikdo nemá odpověď. (5) (6)

Příklad těžby je třeba Bitcoin Block #6667500, který byl vytěžen 21. ledna 2021, ve kterém bylo obsaženo 15853,6 BTC (v té době $505 772 432, při kurzu 21,461 Kč dle kurzovního lístku k danému datu to odpovídá 10 854 382 163,152 Kč v jednom bloku). Uživatel za „vytěžení“ tohoto bloku byl odměněn sítí 6,25 BTC a dalších 0,655 BTC jako poplatek za veškeré transakce v daném bloku. Celkem si tak vydělal $230 008,34 (necelých 5 milionů českých korun). Na stránkách BlockChain.com jsou dostupné veškeré informace o tomto a všech ostatních blocích a transakcích, včetně množství transakcí v jednom bloku, průměrná hodnota transakce, mediánová hodnota transakce a další. (14) (15)

Těžba Bitcoinu se také časem mění a zpomaluje. Na počátku, když byl vytěžen první Bitcoin, byla odměna za vygenerování dalšího bloku 50 BTC. V listopadu roku 2012 byla odměna snížena na polovinu, tedy 25 BTC. Další snížení odměny za vytěžení bloku proběhlo v červnu roku 2016, kdy byla odměna za vytěžení bloku stanovena na 12,5 BTC. Poslední a nejaktuálnější změna proběhla v květnu roku 2020 a odměna je již pouhých 6,25 BTC. Redukce odměny probíhá po vytěžení každého 210 000. bloku, což v průměru vychází na 4 roky. Dle expertů má další půlení proběhnout v květnu 2024. (16) (17)



Obrázek 2 - Odměny těžařů za úspěšné vytěžení bloku (Zdroj: (17), Sabrina Jiang, 2021)

3.3.4 Ekonomické hledisko Bitcoinu

Bitcoin byl v této práci probrán z hlediska tradiční ekonomie, kde bylo zodpovězeno mnoho důležitých otázek. Zbývá odpovědět na jednu, podle autora velice důležitou otázku, kterou je, co by Bitcoin a jeho trh mohlo ohrozit.

Jedna z největších kryptoměnových burz, Coinbase, při svém založení na několik z těchto faktorů poukázala. Při svém založení byla společnost Coinbase povinna předložit svůj business model komisi pro cenné papíry a burzu (SEC v Americe). SEC je regulační orgán zodpovědný za ochranu investorů a poctivého fungování trhů a usnadňování tvorby kapitálu. (18)

V tomto, veřejně dostupném, business modelu je sekce, kde je popsáno, co by mohlo ohrozit investovaný kapitál uživatelů (investorů) platformy. Body, které se týkají Bitcoinu jsou následující:

- Redukce odměn za úspěšné vytěžení bloku
- Odhalení identity Satoshiho Nakamota nebo převedení jeho Bitcoinů z jeho peněženky

- Zákony a regulace ovlivňující Bitcoin negativním způsobem (pokus vlád o centralizaci Bitcoinu)

4 Vlastní práce

4.1 Metodika vlastní práce

Vlastní prací byla těžba Bitcoinu na 3 vybraných aplikacích na základě nastavených parametrů. Po nastavení parametrů a výběru 3 vhodných aplikací pro těžbu, bylo na daných 3 aplikacích těženo stanovenou dobu (pro všechny 3 aplikace identickou) a bylo sledováno, jakou spotřebu měl počítač v průběhu těžby. Po ukončení těžby na všech třech aplikacích byly zpracovány informace, kolik Bitcoinu (po přepočtu) bylo těžbou získáno z každé aplikace, kolik elektřiny bylo těžbou spotřebováno a jakých interních teplot počítače bylo dosaženo. Následně byla přepočítána spotřeba elektřiny na české koruny a bylo vyhodnoceno, zdali je těžba pro běžného člověka s počítačem, jaký má autor, výdělečná nebo prodělečná.

Druhou částí praktické části bylo zjištění, kdy ještě mohla být těžba rentabilní dle parametrů odměny za těžbu v daném roku a průměrné ceně za 1 kWh.

4.1.1 Parametry stanovené pro výběr aplikací

Při výběru těžebního softwaru byl brán ohled na mnohé faktory. Důležité faktory pro autora byly zejména tyto:

- Počáteční investice/Poplatky
- Platforma, na které je software použitelný
- Komplexita užívání softwaru
- Kompatibilita s grafickou kartou
- Software musí umožňovat výplatu v Bitcoinu a přepočet
- Podpora těžby grafickou kartou

4.1.2 Vysvětlení jednotlivých parametrů

Počáteční investice, stejně jako poplatky hrají zásadní roli s ohledem na profitabilitu, tudíž by měly být co nejmenší.

Autor plánuje těžit na svém stolním počítači, který využívá OS Windows 10, proto byl nutný software kompatibilní s Windows 10.

Autor nikdy předtím kryptoměny netěžil a nemá s těžbou žádné zkušenosti. Není uživatelem Linuxu OS, a proto ovládání softwaru příkazovým řádkem pro autora nebylo možností. Požadavkem byla snadná navigace v softwaru a grafické rozhraní.

Některé aplikace se specializují na těžbu pomocí čipů grafických karet pouze od výrobce nVidia, některé jsou kompatibilní pouze s grafickými kartami AMD. (19)

Aplikace bude muset podporovat výplatu v Bitcoinu přímo, aby byly výsledky těžby porovnatelné mezi aplikacemi. Některé aplikace za vás změní těženou měnu za účelem nejvyšší profitability a až konečný výsledek (výplatu) dostanete v Bitcoinu. (19) (20)

Podpora těžby grafickou kartou pro autora byla nutná, protože obecně řečeno je grafická karta nejvýkonnějším komponentem každého běžného počítače, s dedikovanou GPU.

4.1.3 Výběr těžební aplikace (softwaru)

K výběru optimálních tří aplikací byla použita výběrová tabulka. V tabulce se nachází 10 aplikací, které autor našel na 2 serverech a dále si podrobnosti o nich zjišťoval na jejich vlastních webových stránkách.

	Investice	Platforma	Komplexita	Kompatibilita	GPU	Rozhodnutí
CGMiner	0$	Windows	Vysoká	Ne	Ano	Ne
NiceHash	2%	Windows	Nízká	Ne	Ano	Ne
BFGMiner	0$	Windows	Vysoká	Ano	Ano	Ne
CudoMiner	1,5 - 6,5 %	Windows	Nízká	Ano	Ano	Ano
MultiMiner	0$	Windows	Nízká	Ano	Ano	Ne
Kryptex	3%	Windows	Nízká	Ne	Ano	Ne
Ecos	49$	iOS/Android	Nízká	Ne	Není známo	Ne
Awesome	0$	Windows	Nízká	Ano	Ano	Ano
EasyMiner	0$	Windows	Nízká	Ano	Ano	Ne
Gminer	0$	Windows	Vysoká	Ano	Ano	Ano

Tabulka 1 Rozhodovací tabulka pro výběr 3 těžebních aplikací
Zdroj: vlastní zpracování informací dostupných z *(19) (20) (21) (22) (23) (24) (25) (26) (27) (28)*

CGMiner byl vyřazen z výběru, jelikož program je kompatibilní pouze s grafickými kartami (čipy) od výrobce AMD (dříve ATI). Autor vlastní kartu s čipem od výrobce nVidia a z toho důvodu nebude mít možnost program použít. Mimo to je ovládán prostřednictvím příkazového řádku, což není preferováno. (25) (20) (19)

NiceHash by byl ideální kombinací kompatibility, uživatelské přívětivosti a nulového počátečního vstupu. Ovšem vzhledem ke stáří autorova počítače, a především grafické karty využívané k těžbě, není kompatibilní. Dvouprocentní poplatek by byl z případného převodu Bitcoinu na NiceWallet nebo případné externí kryptopeněženky. (19) (20) (29)

U aplikace BFGMiner proběhl pokus o zprovoznění, ovšem přes teoretickou kompatibilitu nefungoval. Proběhl pokus o zprovoznění starších verzí programu, které měly být údajně stabilní, ovšem ani ty nefungovaly. (19) (20) (30) (31) (32)

CudoMiner byl využit, jelikož má grafické rozhraní, webové rozhraní na vzdálené ovládání těžební aplikace. Grafická karta, kterou je autorův stolní počítač vybaven, je podporována. Aplikace má nulové vstupní náklady a poplatky budou odvozeny podle aktivity těžaře a vytěženého množství kryptoměn (v přepočtu na BTC). Poplatek se pohybuje v relaci od 1,5 – 6,5 % celkového výtěžku v posledních 30 dnech. Čím vyšší je vytěžené množství jakékoli podporované kryptoměny, tím jsou menší poplatky. Výtěžek je z jakékoliv kryptoměny přepočítáván do hodnoty Bitcoinu a podle množství vytěžených Bitcoinů jsou odvozeny poplatky. Těžaři odvádí poplatky z výtěžku, ale nikoliv z provedené platby vybrání kryptoměny na jinou externí krypto-peněženku. (33)

Multiminer byl druhou z aplikací, která měla být použita, ovšem mining engine, který měl být používaný touto aplikací je zastaralý a jeho zprovoznění a propojení s aplikací je problematické. Multiminer je software, postavený na těžebním jádru („motoru“ z přímého překladu „mining engine“) softwaru BFGMiner s grafickým rozhraním pro snazší užívání. Není mnoho dostupných informací ohledně vybrání vytěžené kryptoměny, ale v průběhu nastavování aplikace byl těžař obeznámen se vším nastavením této aplikace. (27) (20) (19)

Aplikace Kryptex není kompatibilní s hardwarem autorova počítače. I kdyby byl hardware autorova počítače novější, nejspíše by byla funkčnost problematická, protože Kryptex je specializovaný na dedikovaný těžební hardware. (19)

Ecos je aplikace na cloudovou těžbu, tudíž ani nebyl pro autorův počítač aplikací použitelnou. Pokud by autor s dodavatelem podepsal těžební smlouvu, neměl by kontrolu nad tím, kolik energie pronajatý počítač spotřeboval a kolik stojí jedna Watthodina energie danou společnost. Z důvodu nedostatku kontroly a specializovaného HW služby této společnosti nebudou využity. Cílem práce je ukázat, zdali je těžba kryptoměn rentabilní pro běžného člověka s běžným vybavením. (19) (34)

AwesomeMiner byl využit. Na internetových stránkách nemají informaci o možnosti využití jejich těžební aplikace bezplatně, ovšem po kontaktování podpory byl autor s touto možností obeznámen. (19) (20) (35) (24)

EasyMiner se zdál být ideálním kandidátem pro tuto bakalářskou práci, ale uživatel je nucen těžit Litecoin a má možnost těžit Bitcoin spolu s Litecoinem. Mimo to jsou webové stránky společnosti velice zastaralé a nejasně navigovatelné. Aplikace nebyla z těchto důvodů vybrána. (19) (35)

GMiner byl zvolen pro těžbu i přes svou vyšší komplexnost, neboť další aplikace, které měly teoreticky fungovat, prakticky nefungovaly. S pomocí členů specializovaných komunit zabývajících se těžbou kryptoměn byla aplikace zprovozněna. (28)

4.2 Metody těžby kryptoměn

Proces těžby byl vysvětlen v teoretické části (3.3.3) na příkladu Bitcoinu. Těžba různých kryptoměn se může lišit kryptografickým hashovacím protokolem, ovšem základní idea je stejná. Výpočet matematických příkladů a sítí nastavená obtížnost, kterou musí výsledek výpočtu splňovat.

Metody těžby se liší v komponentech použitých k onomu výpočtu příkladů. Dělí se na CPU mining, GPU mining, ASIC mining a FPGA mining. (36)

4.2.1 CPU Mining

Těžba pomocí procesorů neboli CPU (Central Processing Unit), byla prvotním způsobem získávání Bitcoinu, kde byl využíván veškerý dostupný výkon procesoru nad rámec podpory operačního systému. CPU je výpočetní jednotka, která není specializovaná na žádný typ výpočtu, protože řídí chod počítače a kooperaci jeho komponentů. Výhodou je schopnost rychle vykonávat různorodé výpočty, ovšem kvůli vysoké energetické náročnosti a omezené výpočetní výkonnosti těžba procesorem rychle zastarala. (36) (37)

4.2.2 GPU Mining

GPU – Graphical Processing Unit – grafická procesorová jednotka

GPU mají možnost zpracovávat více vláken informací naráz. Tato vlastnost jim dává určitou výhodu oproti následujícímu typu těžby ASIC. Hlavním úkolem grafických karet je zrychlování vykreslování grafiky a zobrazování vykresleného výsledku na monitoru. Grafické karty jsou běžně vybaveny velkým množstvím ALU jednotek (Arithmetic Logic Unit – aritmeticko-logická jednotka). ALU jsou zodpovědné za matematické výpočty grafických prvků. Díky těmto jednotkám a repetitivnosti výpočtů hashe, ve kterých se mění pouze jedna neznámá (číselné vyjádření obtížnosti výpočtu nastaveného BlockChain sítí), grafické karty v porovnání s procesory v těžbě kryptoměn excelují. (36) (37)

Dnešní nejvýkonnější grafické karty, testované na těžbu kryptoměn, jsou nVidia RTX 3090. Mají hashovací výkon 125–130 MH/s (MegaHash/sekundu) a spotřebují 300 Wattů. 125 MegaHashů je výpočetní výkon v továrním nastavení bez overclockingu. Tato karta má při těžbě Etherea poměr 0,38 Hashrate/Watt. (38) (39)

Přepočet výkonu zmíněné GPU na porovnatelné jednotky: jak bylo v předchozím odstavci zmíněno, předchůdce dnešní nejnovější generace grafických karet má hash rate 125 MegaHashů/s a výkon 300 Wattů (J/s). 125 000 000 Hashů/s lze vydělit 300 Watty (Jouly/s) a vyjde 416 666,7 Hash/J. (Zdroj: vlastní výpočet)

4.2.3 ASIC Mining

ASIC – Application-specific Integrated Circuit – integrovaný obvod specifický pro danou aplikaci / dané užití

ASIC jsou počítače pro jedno specifické užití. Mnoho takových ASIC počítačů je zcela dedikovaných těžbě kryptoměn. Takový ASIC těžební počítač je konstruován a optimalizován pro těžbu jedné specifické kryptoměny. Tedy ASIC pro Bitcoin, je použitelný pouze pro Bitcoin. Vývoj a produkce takových těžebních počítačů je drahá, ovšem efektivita je nesrovnatelně vyšší oproti GPU. (36) (40)

ASIC počítače jsou stavěny čistě s cílem co největšího výpočetního výkonu, kterého dosahují pomocí velkého množství paralelně pracujících jader, mezi které se pipeliningem fragmentuje každá instrukce. Pipelining instrukcí je ideální kooperací softwaru a hardwaru a snaží se neustále zaměstnávat všechna jádra. Každé jádro vykoná fragment vstupní instrukce a tím šetří čas. Pokud jsou jednotlivé části původní instrukce na sobě závislé (musí navazovat), může první jádro v pořadí po dokončení svého fragmentu přijmout další část druhé instrukce, zatímco dokončení první instrukce je přenecháno zbytku jader. Nejlépe tento koncept lze vysvětlit na příkladu ze života, praní prádla. Budeme mít dvě činnosti (procesy), které bude v procesu praní zapotřebí vykonat: praní a sušení. K těmto dvěma procesům budeme mít pračku a sušičku a cyklus obou dvou strojů trvá 30 minut. (41) (42)

S pipeliningem	Pračka	Sušička
0–30 minut	Várka 1	-
30–60 minut	Várka 2	Várka 1
60–90 minut	Várka 3	Várka 2
90–120 minut	-	Várka 3

Tabulka 2 Znázornění časové úspory pipeliningem část 1 – Vlastní zpracování informací dostupných z (41)

Pro znázornění, jak by instrukce byly vykonávány bez pipeliningu budeme mít pračku, která je zároveň vybavena sušičkou. (41)

Bez pipeliningu	Pračka + sušička
0–60 minut	Várka 1
60–120 minut	Várka 2
120–180 minut	Várka 3

Tabulka 3 Znázornění časové úspory pipeliningem část 2 – Vlastní zpracování informací dostupných z (41)

Nejnovější generace ASIC jednotek (Bitcoin Miner S19 Hydro od čínské značky Bitmain), má výpočetní výkon 158 TeraHashů/s a spotřebu 34,5 J/TeraHash. (40) (39)

Přepočet výkonu ASIC jednotky na porovnatelné jednotky: výpočetní výkon udaný v počtu Hashů za sekundu (TeraHashů) a spotřebu energie na TeraHash mezi sebou vynásobíme a získáme počet Joulů za sekundu. Výsledek je 5 451 J/s což je 5 451 W (Wattů). (Zdroj: vlastní výpočet)

Tento výsledek můžeme dosadit do stejné rovnice jako u GPU v kapitole 4.2.2. Výpočetní výkon 158 TH/s (158 * 10^{12} Hash/s) vydělíme výkonem 5451 Wattů. Výsledný poměr počtu vygenerovaných Hashů za 1 Joul energie je 28 985 507 246,3 Hash/J. (Zdroj: vlastní výpočet)

4.2.4 ASIC-odolnost

Existují mince, které ASIC těžbě odolávají. Schopnost kryptoměny odolávat ASIC těžbě spočívá v kódu a konstrukci kryptoměny. Tuto odolnost mají především kryptoměny s typem konsensu PoS, DPoS nebo PoA (Proof-of-Stake, Delegated-Proof-of-Stake a Proof-of-Authority). Jsou to alternativní typy konsensu (kolektivní shody) k PoW, který používá Bitcoin. Ani jedna z alternativních metod nevyžaduje od jednotlivých uzlů sítě, aby využívaly svůj výpočetní výkon. PoW je svou konstrukcí nejbezpečnějším protokolem k dosažení kolektivní shody, ale má své nevýhody. Bitcoin síť má hashrate 286,28 EH/s (286,28 * 10^{18} Hashů/sekundu). S takovým výpočetním výkonem v jedné síti, je prakticky nemožné provést 51% útok. 51% útok je typ kybernetického napadnutí P2P sítě, kdy jedna entita (počítač) vytvoří nadpoloviční většinu virtuálních uživatelů. Každý z těchto virtuálních uživatelů má jiné přihlašovací údaje, nebo jinou IP adresu, tudíž vypadají jako samostatní uživatelé. V momentu, kdy má samotná entita pod kontrolou 51 % legitimně vypadajících uživatelů dané sítě, může provádět neautorizované akce. Konstrukce PoW protokolu je také důvodem jejího, v porovnání s PoS a PoA protokoly, limitovaného množství transakcí za sekundu (TPS – transactions per second). (43) (44) (45) (46) (47)

Některé populární kryptoměny získaly díky svým komunitám své ASIC-resistant odnože (forks), které jsou i v dnešní době těžitelné grafickými kartami, jako třeba Bitcoin Gold (BTG).

4.2.5 FPGA Mining

FPGA – Field-Programmable Gate Array (Konfigurovatelné číselné integrované obvody)

FPGA jsou méně výkonnou, ale více flexibilní verzí ASIC počítačů. Jsou určeny pro těžbu kryptoměn, které vyžadují velké množství výpočetního výkonu. V porovnání s ASIC počítači jsou méně výkonné, mají menší spotřebu energie, ovšem také mají menší poměr výpočetního výkonu na jeden Joul energie. Co se výkonu týče, jsou tedy podřadné ASIC počítačům, ale jejich velkou výhodou je fakt, že nejsou limitovány na jednu specifickou kryptoměnu. Uživatelsky jsou velice nepřívětivé, ale pokud je někdo znalý programování a problematiky kryptoměn, může si naprogramovat FPGA počítač na těžbu jakékoli kryptoměny na jakémkoli algoritmu. (48) (49) (50)

Pro kryptoměny jako je Bitcoin jsou tedy na pomyslném vrcholu stále ASIC počítače, ovšem nevýhodou je, že těžař se v momentu koupě oddává těžbě dané kryptoměny na několik dalších let. (48) (49)

4.2.6 Porovnání těžebních metod

V dnešní době jsou použitelné 3 z uvedených 4 metod. Těžba procesorem je již zcela nerentabilní a tím pádem se již nepoužívá. Těžba grafickou kartou se stále u některých velkých kryptoměn používá, ovšem využití najde spíše u menších kryptoměn. Malou kryptoměnou je míněna taková kryptoměna, jejíž síť má malý výpočetní výkon, a tudíž menší konkurenci, nebo kryptoměny, které nejsou stavěny na protokolu PoW. ASIC těžba je dnes nejvíce profitabilní metodou, ovšem vstupní náklady jsou tak vysoké, že si běžný těžař ASIC počítač nepořídí. ASIC těžba je určena pro lidi/firmy, které se těžbou kryptoměn živí. FPGA těžba je méně profitabilní, ovšem i méně finančně náročná a má menší vstupní náklady. Porovnat FPGA minery s ASIC minery je složité, protože mnohdy FPGA minery jsou využívané pro těžbu ASIC-resistant kryptoměn, ovšem nejsou konstruovány na těžbu kryptoměn, které povolují ASICy, jelikož v takovém případě ASICy mají zcela jistou dominanci.

4.3 „Těžební bazény“

Mining pool neboli těžební bazén je uskupení velkého množství těžařů v jeden celek, ve kterém je spojen veškerý nashromážděný výpočetní výkon. Tato uskupení jsou formována za

účelem zvýšení konkurenceschopnosti na těžebním „trhu“. Motivací těžařů pro připojení se do nějakého z bazénů, je zvýšení šance na odměnu. Šance na odměnu se zvyšují, ale výše odměny se drasticky snižuje, přesto bazénů všichni využívají. Bazény se kromě typu distribuce odměny mohou lišit i ve faktu, zdali rozdělují i transakční poplatky, nebo zdali si transakční poplatky nechá správce bazénu pro sebe.

Podíl v těžebním bazénu je metoda, na základě které je pak rozdělována odměna mezi jednotlivé těžaře, pakliže daný bazén uspěje v těžbě bloku. Jeden podíl je jedno navrhnuté řešení nové adresy bloku. Následný výpočet odměny těžaře už velice záleží na typu bazénu. Velké zaběhnuté bazény mají také výhodu kapitálu, který mnohdy investují do webového rozhraní, skrze které mnohdy mohou být těžební počítače ovládány na dálku a mohou být měřeny faktory jako výpočetní výkon (hashrate), teplota těžící jednotky, spotřeba elektřiny (W) a případné předpovědi měsíčního výtěžku. (51) (52)

Typů těžebních bazénů je, dle metody rozdělování odměny mezi své těžaře přes 10, ovšem pro tuto práci jsou zmíněné základní a nejvíce užívané. (53)

Proporční bazény jsou jedním z nejčastějších typů. V tomto typu bazénu jsou těžaři sbírány podíly, dokud není bazénem úspěšně vytěžen nový blok. Následně je odměna (k datu 28. března 2023) 6,25 BTC za jeden vytěžený blok a některé bazény k tomu přičtou částku nakumulovanou z poplatků za transakce, zahrnuté v daném vytěženém bloku. Úspěšný těžař bloku 777162 byl odměněn standartní odměnou ve výši 6,25 BTC navýšenou o 0,2334 BTC jako poplatek za veškeré transakce. (51) (52) (53) (54)

Pay-per-Share (PPS) bazény mají stanovené fixní množství podílů, při kterých by teoreticky měl být vytěžen blok. V takovém bazénu se mnohdy odečítá poplatek, který si bere bazén za zprostředkování vyšší šance a může se přičítat adekvátní podíl za transakční poplatky. V případě PPS bazénu těžař odevzdává největší procento svého výtěžku jako poplatek za využití daného bazénu. Ostatní bazény mají běžně 1-2 % jako poplatek bazénu, zatímco PPS a jeho modifikace mají 4-5 % poplatek. Důvodem navýšeného poplatku je fakt, že bazény PPS a jeho modifikované verze vyplácejí poplatky svým těžařům, i když daný bazén nevytěží blok. Modifikovanými verzemi PPS jsou PPS+ a FPPS, které k samotné odměně za vytěžení bloku přidávají i odměnu v podobě transakčních poplatků. Pro těžaře je výhodnější těžit v modifikovaných verzích PPS+ a FPPS. (51) (52) (53) (55) (56)

Pay-per-Last-N-shares (PPLNS) se v porovnání s PPS liší v tom, že pokud daný bazén nevytěží blok, těžaři nejsou odměněni. Těžaři, kteří si vyberou jeden bazén a v tom jsou

dlouhodobě, jsou odměňováni více než těžaři, kteří skáčou mezi bazény. PPLNS při vyhodnocení jsou započteny i podíly z minulého, úspěšného, vytěženého bloku a ty jsou přičteny ke stávajícím podílům. Tato metoda vyplácení těžařů snižuje risk operátora bazénu. Nemusí vyplácet těžařům, pokud není nalezen blok, což umožňuje mít nižší poplatky za členství v bazénu. (56)

Bazén sólové těžby se chová a funguje stejně jako jakýkoli jiný bazén, ovšem má jen jednoho těžaře, kterému je přidělena celá odměna v případě, že se tomu bazénu povede vytěžit blok. (53)

Pooled mining (sdružená těžba) je systém výplaty, ve kterém je starším podílům (z dřívější části bloku) přiřazena nižší váha, než novějším (z pozdější části bloku). Tento systém má těžaře odradit od skákání mezi bazény. V momentě rozdělování odměn pooled mining funguje jako proporční s váhami jednotlivých podílů. Byl poprvé použit v roce 2010 bazénem SlushPool. (53)

Geometrická metoda (GM) byla založena na stejném nápadu, jako Pooled mining metoda, ovšem „váha“ je stejná pro každý podíl, nezávisle na momentu, ve kterém byl podíl získán v rámci těžby dalšího nového bloku. V této metodě tedy nejsou zvýhodněny novější podíly nad staršími ani naopak. (53)

4.4 Výběr těžebního bazénu

Požadavky na těžební bazény byly nastaveny následovně:

- Musí být typu PPS, PPS+ nebo FFPS, aby autor s nízkým výpočetním výkonem měl zajištěný alespoň nějaký výtěžek.
- Musí mít webové prostředí, které výtěžek ukáže.
- Musí mít rozhraní, které autorovi ukáže výtěžek, i když by těžil externí aplikací.

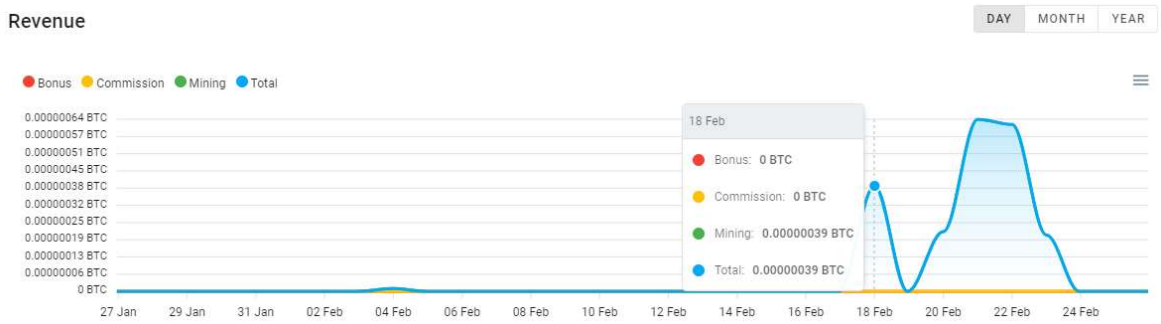
Aplikace CudoMiner, na které bylo v průběhu práce těženo, poskytuje i svůj vlastní bazén, do kterého se lze připojit i externími těžebními aplikacemi, poskytuje grafické znázornění výtěžků a je typu PPS. Proto byl jejich bazén vybrán jako vhodný i pro těžbu na zbylých dvou těžebních aplikacích.

4.4.1 Výsledky těžby

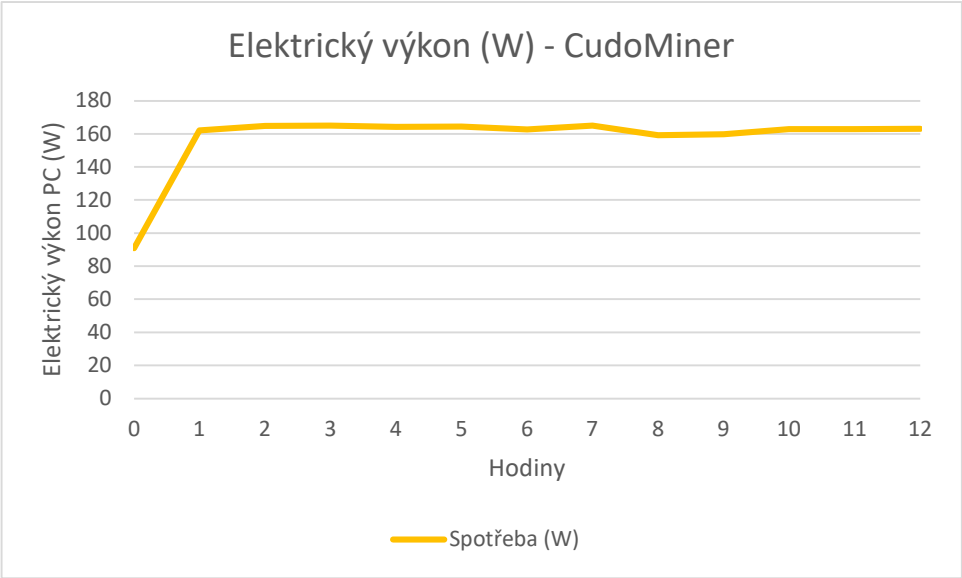
Pro zachování objektivity byl pořízen digitální měřič elektrické spotřeby Solight DT26. Před těžbou na každé ze tří aplikací byl měřič resetován. Pro účely výpočtu rentability byly používány průměrné roční hodnoty ceny za 1 kWh elektřiny. Každá těžba trvala 12 nepřetržitých hodin a každou hodinu byly snímány: hodnoty vytížení grafické karty, teplota grafické karty a elektrický výkon počítače v daný moment. Celkové množství spotřebované elektřiny bylo naměřeno ihned po ukončení procesu těžby. Veškeré výpočty jsou vztahovány ke kurzu Bitcoinu z 26.2.2023. Je nutné brát v potaz, že trh s kryptoměnami je velice volatilní a je ovlivňován mnohými faktory.

4.4.2 CudoMiner

CudoMiner byla první aplikace použita k těžbě, výtěžek z této aplikace za 12 hodin je vy výši 0,00000039 BTC a celková elektrická spotřeba byla 1,9 kWh.



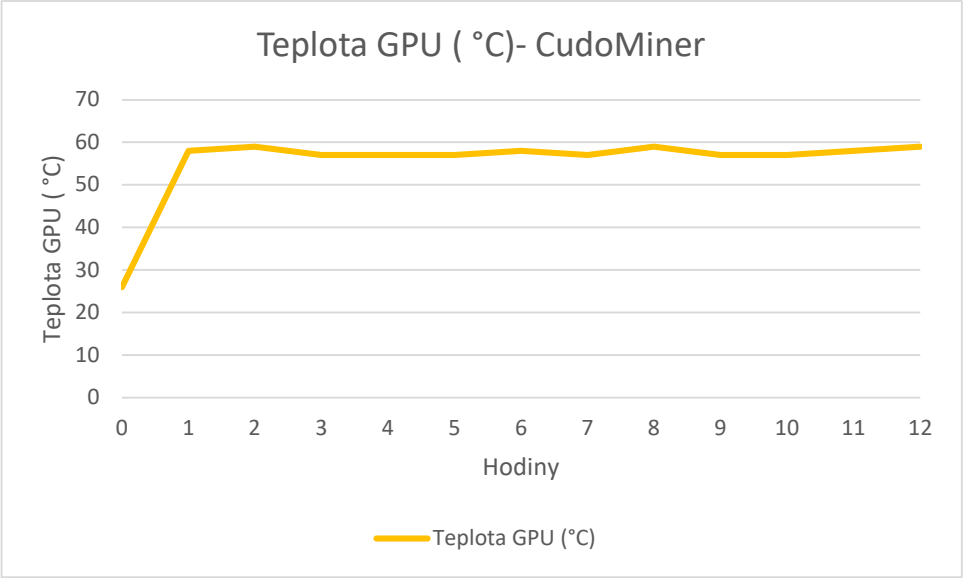
Obrázek 3 Výtěžek z CudoMiner zobrazený v CudoDashboard Revenue grafu (57)



Graf 1 Elektrický výkon PC při těžbě na CudoMiner

Zdroj: vlastní zpracování naměřených dat

Spotřeba počítače byla při těžbě stabilní, pohybovala se kolem 163 W s odchylkami +2 W -3 W a průměrnou hodnotou 162,99W. V klidovém režimu před započetím těžby byla spotřeba 90,9 W. Spotřeba v průměru vzrostla o 79,309 % oproti klidovému režimu.



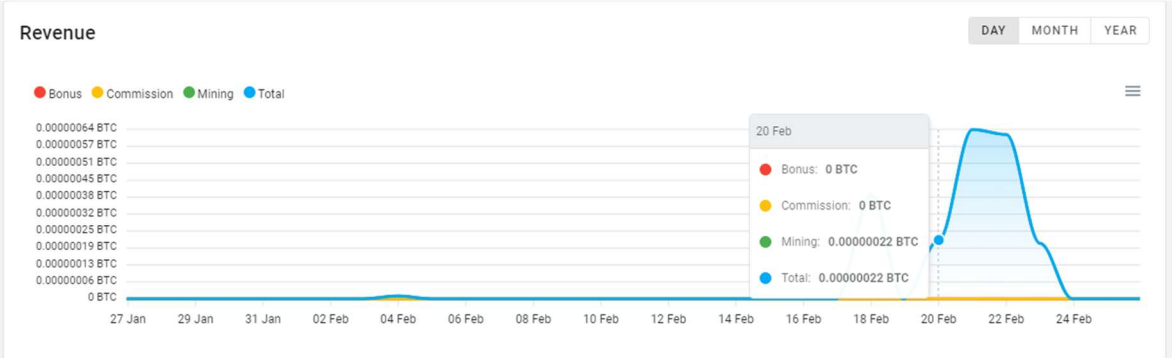
Graf 2 Teplota GPU při těžbě na CudoMiner

Zdroj vlastní zpracování naměřených dat

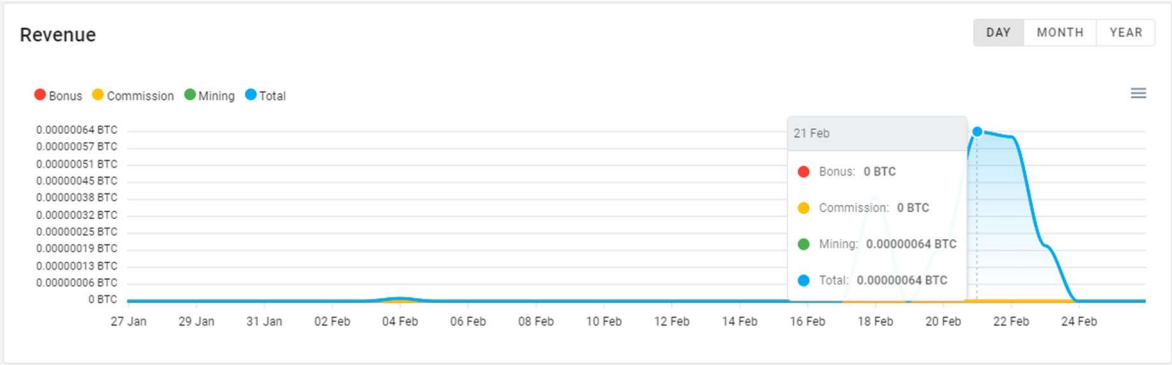
Před započetím těžby byla aplikací NZXT CAM naměřena teplota grafické karty 26 °C. V průběhu těžby se teplota grafické karty pohybovala v rozsahu 57–59 °C s průměrnou teplotou 57,75 °C. Vytížení grafické karty bylo před započetím těžby na úrovni 5 %, po započetí těžby vytížení stouplo na 100 % a až do konce těžby nekleslo ani o jeden procentní bod. Byl zaznamenán průměrný teplotní nárust o 122,115 % oproti klidovému režimu.

4.4.3 AwesomeMiner

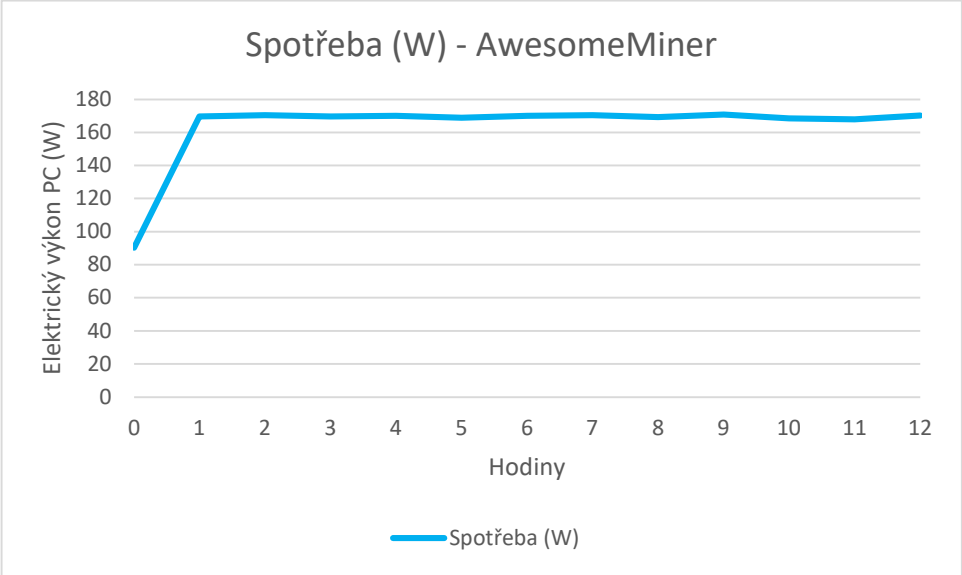
Výtěžek z aplikace AwesomeMiner byl celkem 0,00000086 BTC s celkovou spotřebou 2 kWh. Těžba byla zahájena v 20:15 a proto je výtěžek v grafu rozdělen do dvou dnů.



Obrázek 4 Výtěžek 1/2 z AwesomeMiner zobrazený v CudoDashboard Revenue grafu (57)



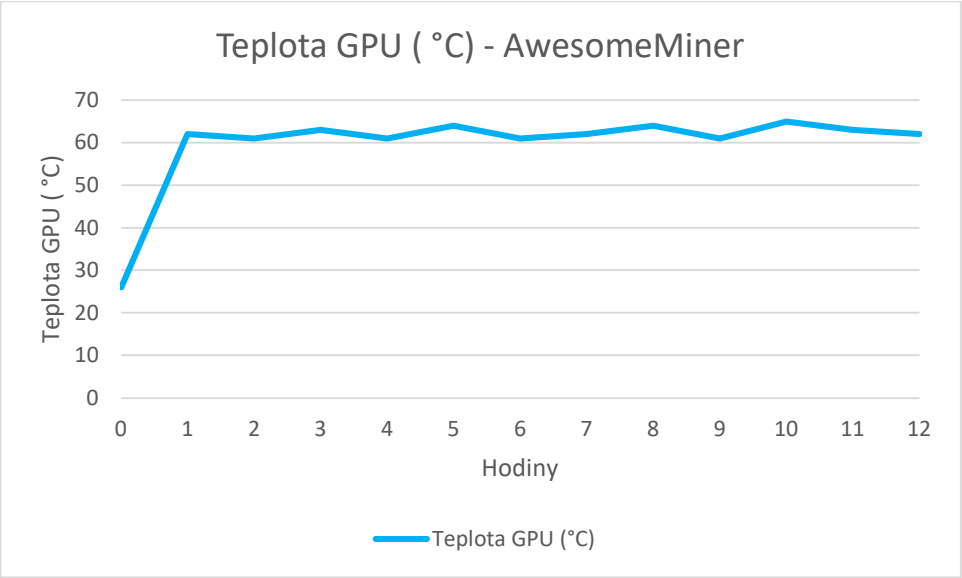
Obrázek 5 Výtěžek 2/2 z AwesomeMiner zobrazený v CudoDashboard Revenue grafu (57)



Graf 3 Elektrický výkon PC při těžbě na AwesomeMiner

Zdroj: vlastní zpracování naměřených dat

Spotřeba počítače byla při těžbě stabilní, pohybovala se kolem 169 W s odchylkami +- 1 W a průměrnou hodnotou 169,575 W. V klidovém režimu před započetím těžby byla spotřeba 90,3 W. Spotřeba v průměru vzrostla o 87,791 % oproti klidovému režimu.



Graf 4 Teplota GPU při těžbě na AwesomeMiner

Zdroj: vlastní zpracování naměřených dat

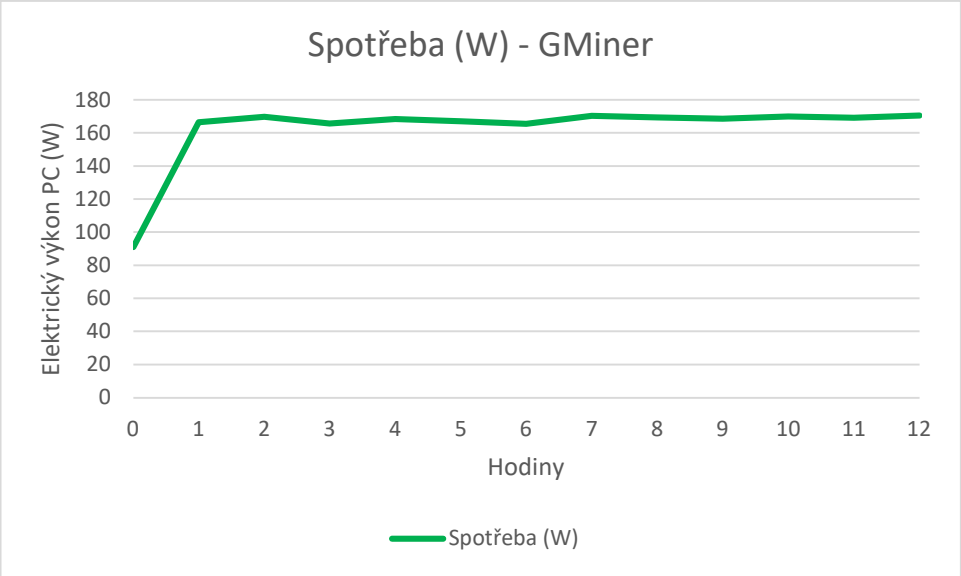
Před započetím těžby byla aplikací NZXT CAM naměřena teplota grafické karty 26 °C. V průběhu těžby se teplota grafické karty pohybovala v rozsahu 61–65 °C s průměrnou teplotou 62,42 °C. Vytížení grafické karty bylo před započetím těžby na úrovni 5 %, po započetí těžby vytížení stouplo na 100 % a až do konce těžby nekleslo ani o jeden procentní bod. Byl zaznamenán průměrný teplotní nárust o 140,064 % oproti klidovému režimu.

4.4.4 GMiner

Výtěžek z aplikace GMiner byl celkem 0,00000083 BTC s celkovou spotřebou 1,9 kWh. Těžba byla zahájena v 15:07 a proto je výtěžek v grafu rozdělen do dvou dnů.

Obrázek 6 Výtěžek 1/2 z GMiner zobrazený v CudoDashboard Revenue grafu (57)

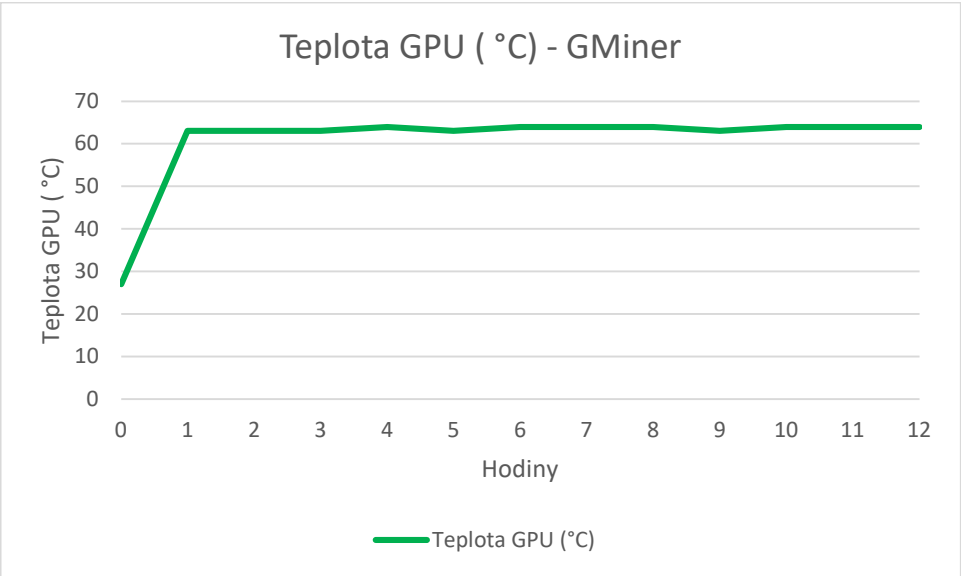
Obrázek 7 Výtěžek 2/2 z GMiner zobrazený v CudoDashboard Revenue grafu (57)



Graf 5 Teplota GPU při těžbě na AwesomeMiner

Zdroj: vlastní zpracování naměřených dat

Spotřeba počítače byla při těžbě stabilní, pohybovala se kolem 168 W s odchylkami +2 W -3 W a průměrnou hodnotou 168,375 W. V klidovém režimu před započetím těžby byla spotřeba 91,1 W. Spotřeba v průměru vzrostla o 84,824 % oproti klidovému režimu.



Graf 6 Teplota GPU při těžbě na GMiner

Zdroj: vlastní zpracování naměřených dat

Před započetím těžby byla aplikací NZXT CAM naměřena teplota grafické karty 27 °C. V průběhu těžby se teplota grafické karty pohybovala v rozsahu 62–64 °C s průměrnou teplotou 63,58 °C. Vytížení grafické karty bylo před započetím těžby na úrovni 6 %, po započetí těžby vytížení stouplo na 100 % a až do konce těžby nekleslo ani o jeden procentní bod. Byl zaznamenán průměrný teplotní nárust o 135,494 % oproti klidovému režimu.

5 Výsledky

5.1 Vyhodnocení nejlepší aplikace dle rentability

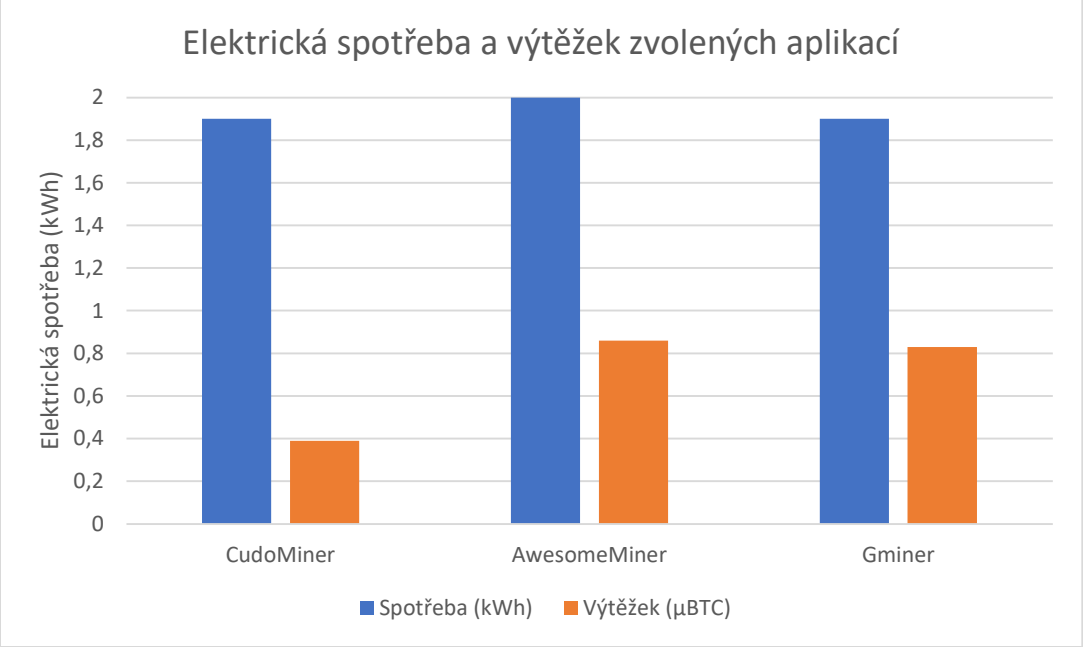
Rentabilita bude vypočítána s průměrnou cenou elektřiny 3,629 Kč/kWh (k datu 23.2.2023) a kurzem 1 BTC = 521 140,62 Kč (k datu 26.2.2023). (58)

CudoMiner přinesl výtěžek 0,00000039 BTC, na koruny přepočteno 0,20324 Kč a bylo spotřebováno 1,9 kWh. Spotřeba elektřiny přepočtena na koruny je 6,8951 Kč.

AwesomeMiner přinesl výtěžek 0,00000086 BTC, na koruny přepočteno 0,44818 Kč a bylo spotřebováno 2 kWh. Spotřeba elektřiny přepočtena na koruny je 7,258 Kč.

GMiner přinesl výtěžek 0,00000083 BTC, na koruny přepočteno 0,43254 Kč a bylo spotřebováno 1,9 kWh. Spotřeba elektřiny přepočtena na koruny je 6,8951 Kč.

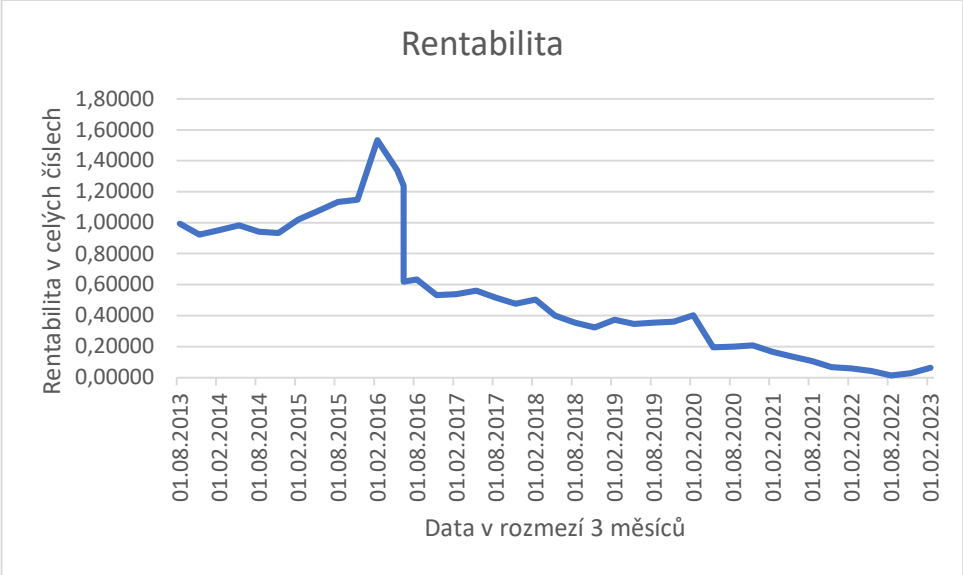
Žádná z aplikací při daném výpočetním výkonu, momentálním kurzu Bitcoinu a ceně elektřiny není rentabilní. CudoMiner je co se výdělku týče nejhorší, přinese (při výše uvedených kurzech) 0,02800 Kč výtěžku za každou korunu utracenou na elektřině. Aplikací na druhé příčce je AwesomeMiner, který za každou korunu utracenou na elektřině (při výše uvedených kurzech) přinese výtěžek ve výši 0,06174 Kč. Nejlepší aplikací na těžbu co se rentability týče je tedy GMiner, který vytěží zlomky bitcoinu ve výši 0,06273Kč (při výše uvedených kurzech) za každou korunu utracenou za elektřinu. V grafu bylo využito jednotek mikrobitcoin (µBTC) za účelem snazší grafické reprezentace výsledků.



Graf 7 Zobrazení spotřeby elektřiny a výtěžku u každé aplikace

Zdroj: vlastní zpracování naměřených dat

Nejlepší aplikací je GMiner z hlediska rentability, ovšem v dnešní době je rentabilita těžby neprofitabilní. Hlavní otázkou je, kdy ještě těžba grafickými kartami byla rentabilní? Zcela jistě byla rentabilní ještě v roce 2013, než se do procesu těžby Bitcoinu zapojily i ASIC počítače. Proměnné, které se mění v čase, je cena elektřiny a velikost odměny za vytěžení nového bloku. Proměnných je více, jako třeba cena samotného Bitcoinu, ale bude počítáno s cenou uvedenou v kapitole 5.1. V časové ose se budeme pohybovat po 3měsíčních intervalech.



Graf 8 Rentabilita těžby napříč časem

Zdroj: vlastní zpracování naměřených dat a dat z: (58)

Těžba autorovým počítačem by byla rentabilní v období mezi 23. únorem 2015 až do období druhého půlení odměny za vytěžení bloku Bitcoinu, které proběhlo 9. června 2016.

5.2 Dopad na životní prostředí

V případě těžby na autorově počítači byl zaznamenán nárust teploty grafické karty (těžební jednotky) na 222,115 % u aplikace CudoMiner, na 240,064 % u aplikace AwesomeMiner a na 235,494 % klidové teploty u aplikace GMiner. Na autorově systému tak byl naměřen průměrný nárust o 132,558 % (na 232,558 %) klidové teploty grafické karty.

Centrum alternativních financí Cambridgeské univerzity dedikovalo Bitcoinu stránku, na které jsou mapovány mnohé ekologické faktory, jako elektrická spotřeba celé sítě Bitcoinu, emise skleníkových plynů sítě Bitcoinu, mapují, kde se ve světě nachází jaké procento

výpočetního výkonu. Mapa může být zkreslená využíváním VPN služeb, které přesměrují komunikaci přes virtuální bod a daný počítač. Ačkoliv je fyzicky v Praze, v rámci internetu se tváří, že je například v Irsku. Stránky s elektrickou spotřebou a emisemi skleníkových plynů sítě Bitcoinu jsou každých 24 hodin aktualizovány. Data týkající se emisí skleníkových plynů byly rozčleněny. Na nejlepší scénář: veškeré elektrické potřeby sítě Bitcoinu by byly pokryty elektřinou produkovanou vodními elektrárnami. V takovém případě by síť Bitcoinu za rok vyprodukovala 2,46 Megatun ekvivalentu oxidu uhličitého ($MtCO_2e$). Reálný odhad byl vypočítán na základě poměrů globální produkce elektřiny různými způsoby (např. vodní, větrná, jadrná, spalovací elektrárna). Tento odhad je roční produkce 59,42 $MtCO_2e$. Nejhorším scénářem z ekologického hlediska by bylo, kdyby veškeré operace sítě Bitcoinu byly kryty elektřinou vyprodukovanou spalováním uhlí. V takovém případě by síť Bitcoinu vyprodukovala 117,38 $MtCO_2e$. Za rok 2021 vyprodukovala síť Bitcoinu 56,29 $MtCO_2e$. V České republice připadalo v roce 2021 na jednoho obyvatele 9,24 tuny ekvivalentu oxidu uhličitého. Tato hodnota byla vynásobena počtem obyvatel z roku 2021 a roční produkce ekvivalentu oxidu uhličitého České republiky za rok 2021 vyšla 97,16 $MtCO_2e$. V případě Švýcarska vyšel výsledek 34,99 $MtCO_2e$ za rok 2021. Samotná síť Bitcoinu vyprodukuje za rok porovnatelné množství emisí skleníkových plynů, jako menší vyspělé evropské státy. (59) (60) (61) (62) (63)

Stejně jako data týkající se skleníkových plynů vyprodukovaných těžbou Bitcoinu, tak i data o elektrické spotřebě sítě Bitcoinu jsou na stránkách Cambridgské univerzity každodenně aktualizovány. Minimální teoretická hranice spotřeby elektřiny sítí Bitcoinu je (k datu 27.2.2023) 6,41 GW, odhadovaná spotřeba elektřiny je 13,38 GW a maximální teoretická hranice spotřeby elektřiny je 22,21 GW. Pro vyjádření elektrické spotřeby za den musí tato čísla být vynásobena počtem hodin ve dni. Minimální teoretická hranice denní spotřeby elektřiny vyšla na 153,84 GWh/den, odhadovaná denní spotřeba vyšla 321,12 GWh/den a maximální hranice denní spotřeby vyšla 553,04 GWh/den. Tato čísla byla dále vynásobena počtem dní v roce, čímž byla získána roční spotřeba sítě Bitcoinu. Odhadovaná roční elektrická spotřeba sítě Bitcoinu je 117,26 TWh s teoretickým rozsahem 56,23–194,67 TWh. Po sečtení čtvrtletních hodnot „Tuzemská brutto spotřeba [GWh]“ byla získána hodnota roční elektrické spotřeby České republiky 70 928,5 GWh/rok, což se rovná 70,9285 TWh/rok. Odhadovaná roční spotřeba je téměř identická jako odhadovaná roční spotřeba Spojených Arabských Emirátů a porovnatelná s odhadovanou roční spotřebou států jako je Argentina, Norsko, Švédsko a sousední Polsko (64) (65) (66) (67) (68) (69)

6 Závěr

Bakalářská práce byla věnována kryptoměnám, které ačkoli existují již relativně dlouhou dobu, jsou stále aktuální. Vzhledem k nejnovějšímu dění se dokonce stávají stále aktuálnějšími. Čína si například založila svou vlastní národní, centralizovanou kryptoměnu. Celý svět hledá způsob, jak kryptoměny zakomponovat do svého každodenního chodu a jak je a jejich technologie využít k lepšímu fungování stávajících systémů.

Výstupem autorovy práce je fakt, že v dnešní době se s jistotou nevyplatí těžit Bitcoin běžným počítačem, pokud záměrem těžby je okamžitý profit. Trh s kryptoměnami je velice volatilní, a ještě navíc ovlivněn momentální recesí. Kombinace vysokých cen elektřiny a nízkých cen kryptoměn (relativní vyjádření vůči historickým hodnotám kryptoměn) je důvodem, proč se nevyplatí těžit, pokud těžař chce mít profit okamžitě. Těžba by v autorově případě nebyla profitabilní ani v případě, že bychom za cenu Bitcoinu dosadili historicky nejvyšší hodnotu. Z externích zdrojů bylo zjištěno, že dopad na životní prostředí pouze jedné jediné kryptoměny je porovnatelný s dopadem některých vyspělých zemí. Autor na to konto tvrdí, že kryptoměny jako celek mají nezanedbatelný dopad na životní prostředí.

7 Seznam použitých zdrojů

1. Kasperky. *What is cryptocurrency and how does it work?* [Online] Kaspersky, 12. Červenec 2018. [Citace: 22. Září 2022.] https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency.
2. Dominin Stroukal, Jan Skalický. *Bitcoin a jiné kryptopeníze budoucnosti.* Praha : Grada Publishing, 2021. 9788027110438.
3. Laurence, Tiana. *Blockchain For Dummies.* místo neznámé : John Wiley & Sons Inc, 2019. ISBN: 978-1-119-54601-6 (ebk).
4. Blockchain.com. *Blockchain.* [Online] Blockchain, 29. Červen 2022. [Citace: 29. Červen 2022.] https://www.blockchain.com/btc/tx/1df43a64f8332788d649afaa1ab1b9dfae206bedc435208f7fd833d2b1b4be74.
5. Frankfield, Jake. Investopedia. *Proof of Work (PoW).* [Online] Investopedia, 2. Květen 2022. [Citace: 10. Říjen 2022.] https://www.investopedia.com/terms/p/proof-work.asp.
6. Frankenfield, Jake. Investopedia. *Bitcoin Mining.* [Online] Investopedia, 14. Červenec 2021. [Citace: 8. Říjen 2022.] https://www.investopedia.com/terms/b/bitcoin-mining.asp.
7. Kriptomat. *A Brief History of Blockchain Technology That Everyone Should Read.* [Online] Kriptomat, 17. Březen 2022. [Citace: 21. Září 2022.] https://kriptomat.io/blockchain/history-of-blockchain/.
8. Kevin Voigt, Andy Rosen. nerdwallet. *What is Blockchain? Blockchain Technology, Explained.* [Online] nerdwallet, 25. Červen 2021. [Citace: 20. Září 2022.] https://www.nerdwallet.com/article/investing/blockchain.
9. penize.cz. *Hyperinflace v Německu 1923.* [Online] 27. Září 2003. [Citace: 23. Říjen 2022.] https://www.penize.cz/15896-hyperinflace-v-nemecku-1923.
10. Carlogos.org. *10 Rarest cars in the world.* [Online] 8. Září 2020. [Citace: 23. Říjen 2022.] https://www.carlogos.org/reviews/rarest-cars-in-the-world.html.
11. Kurzy.cz. *USD průměrné kurzy 2018, historie kurzů měn.* [Online] [Citace: 23. Říjen 2022.] https://www.kurzy.cz/kurzy-men/historie/USD-americky-dolar/2018/.
12. Graf Bitcoin k USD. *CoinMarketCap.* [Online] 9. Květen 2013. [Citace: 29. Červen 2022.] https://coinmarketcap.com/cs/currencies/bitcoin/.
13. Number of Bitcoins in circulation worldwide from October 2009 to 2022. *Statista.* [Online] Statista, 30. Leden 2009. [Citace: 29. Červen 2022.] https://www.statista.com/statistics/247280/number-of-bitcoins-in-circulation/.
14. Blockchain Block #667000. *Blockchain.* [Online] Blockchain. [Citace: 8. Říjen 2022.] https://www.blockchain.com/btc/block/667000.
15. Kurzy historie, kurzovní lístek ČNB 21.1.2021, historie kurzů měn. *Kurzy.* [Online] Kurzy, 1. Leden 2021. [Citace: 8. Říjen 2022.] https://www.kurzy.cz/kurzy-men/historie/ceska-narodni-banka/D-21.1.2021/.
16. Whittaker, Matt. Why is bitcoin halving. *Forbes.* [Online] Forbes, 22. Červenec 2022. [Citace: 29. Říjen 2022.] https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin-halving/.
17. Hong, Euny. How does bitcoin mining work? *Investopedia.* [Online] 5. Květen 2022. [Citace: 29. Říjen 2022.] https://www.investopedia.com/tech/how-does-bitcoin-mining-work/.
18. Chen, James. Securities and Exchange Commission (SEC) Defined, How It Works. *Investopedia.* [Online] 27. Duben 2022. [Citace: 29. Říjen 2022.] https://www.investopedia.com/terms/s/sec.asp.
19. Wade, Jacob. Money.com. *9 Best Bitcoin Mining Software of 2023.* [Online] 26. Prosinec 2022. [Citace: 10. Leden 2023.] https://money.com/best-bitcoin-mining-software/.

20. Kurko, Michael. Investopedia. *Best Bitcoin Mining Software.* [Online] Investopedia, 3. Leden 2023. [Citace: 10. Leden 2023.] 9 Best Bitcoin Mining Software of 2023.
21. Kryptex. *The Best GPUs for Mining.* [Online] Kryptex, 11. Leden 2023. [Citace: 11. Leden 2023.] https://www.kryptex.com/en/best-gpus-for-mining.
22. NiceHash. *Is my hardware supported?* [Online] NiceHash. [Citace: 11. Leden 2023.] https://www.nicehash.com/support/mining-help/general-help/is-my-hardware-supported.
23. easyminer. *Easyminer FAQ.* [Online] [Citace: 10. Leden 2023.] https://www.easyminer.net/faq/.
24. awesomeminer. *Frequently asked questions.* [Online] awesomeminer. [Citace: 10. Leden 2023.] https://support.awesomeminer.com/support/solutions/.
25. cgminer.info. *CGMiner.* [Online] [Citace: 11. Leden 2023.] https://cgminer.info/.
26. cudominer. *What coins does Cudo Miner support?* [Online] cudominer. [Citace: 10. Leden 2023.] https://www.cudominer.com/kb/what-coins-does-cudo-miner-support/.
27. nwools. *MultiMiner.* [Online] [Citace: 11. Leden 2023.] https://nwoolls.github.io/MultiMiner/.
28. GitHub. *GMinerRelease.* [Online] GitHub, 5. Únor 2023. [Citace: 22. Únor 2023.] https://github.com/develsoftware/GMinerRelease/releases.
29. NiceHashSupport. *Service fees for miners.* [Online] https://www.nicehash.com/support/mining-help/earnings-and-payments/service-fees-for-miners.
30. Jr, Luke. github. *luke-jr/bfgminer.* [Online] github, 26. Srpen 2021. [Citace: 12. Leden 2023.] https://github.com/luke-jr/bfgminer.
31. BitcoinStackExchange. *Setting up BFGMiner with Devices.* [Online] 10. Březen 2016. [Citace: 12. Leden 2023.] https://bitcoin.stackexchange.com/questions/17063/setting-up-bfgminer-with-devices.
32. manpages. *bfgminer.* [Online] [Citace: 12. Leden 2023.] https://manpages.org/bfgminer.
33. cudominer. *Pricing and fees.* [Online] cudominer. [Citace: 12. Leden 2023.] https://www.cudominer.com/pricing/.
34. ECOS FAQ. *ecos.am.* [Online] Ecos. [Citace: 13. Leden 2023.] https://ecos.am/en/faq#/.
35. awesomeminer. *Awesome Miner subscription.* [Online] [Citace: 13. Leden 2023.] https://support.awesomeminer.com/support/solutions/.
36. academy.binance. *How to mine cryptocurrency?* [Online] 23. Prosinec 2022. [Citace: 14. Leden 2023.] https://academy.binance.com/en/articles/how-to-mine-cryptocurrency.
37. Seth, Shobhit. investopedia. *GPU Usage in Cryptocurrency Mining.* [Online] Investopedia, 18. Duben 2022. [Citace: 13. Leden 2023.] https://www.investopedia.com/tech/gpu-cryptocurrency-mining/.
38. Henderson, Amanda. Best Mining GPU (Graphics Card) for Bitcoin & Ethereum in 2023. *guru99.* [Online] 17. Prosinec 2022. [Citace: 14. Leden 2023.] https://www.guru99.com/best-mining-gpus.html.
39. Wade, Jacob. Investopedia. *Hash Rate.* [Online] Investopedia, 6. Říjen 2022. [Citace: 15. Leden 2023.] https://www.investopedia.com/hash-rate-6746261.
40. Tardi, Carla. Investopedia. *Application-Specific Integrated Circuit (ASIC) Miner.* [Online] Investopedia, 27. Září 2022. [Citace: 13. Leden 2023.] https://www.investopedia.com/terms/a/asic.asp.
41. Xiang, Dave. youtube. *What Is Instruction Pipelining?* [Online] Youtube, 16. Březen 2016. [Citace: 16. Leden 2023.] https://www.youtube.com/watch?v=2Crvy_cj5s4&ab_channel=DaveXiang.
42. LearnByBit. *What Are ASIC-resistant Cryptocurrencies?* [Online] 19. Duben 2022. [Citace: 16. Leden 2023.] https://learn.bybit.com/crypto/what-are-asic-resistant-cryptocurrencies/.

43. Ma, John. academy.binance. *ASIC-resistant.* [Online] Binance. [Citace: 16. Leden 2023.] https://academy.binance.com/en/glossary/asic-resistant.
44. Coinwarz. *Bitcoin Hashrate Chart.* [Online] [Citace: 16. Leden 2023.] https://www.coinwarz.com/mining/bitcoin/hashrate-chart.
45. academy.binance. *What Is Proof of Stake (PoS)?* [Online] Binance, 12. Prosinec 2022. [Citace: 16. Leden 2023.] https://academy.binance.com/en/articles/proof-of-stake-explained.
46. academy.binance. *Delegated Proof of Stake Explained.* [Online] Binance, 28. Prosinec 2022. [Citace: 16. Leden 2023.] https://academy.binance.com/en/articles/delegated-proof-of-stake-explained.
47. academy.binance. *Proof of Authority Explained.* [Online] Binance, 12. Leden 2023. [Citace: 16. Leden 2023.] https://academy.binance.com/en/articles/proof-of-authority-explained.
48. LetsExchange. *FPGA Mining vs ASIC Mining: What Is More Profitable?* [Online] LetsExchange, 12. Leden 2022. [Citace: 8. Únor 2023.] https://letsexchange.io/blog/fpga-mining-vs-asic-mining-what-is-more-profitable/.
49. Medium. *Cryptocurrency Mining: Why Use FPGA for Mining? FPGA vs GPU vs ASIC Explained.* [Online] Medium, 27. Červen 2019. [Citace: 8. Únor 2023.] https://medium.com/fpga-guide/cryptocurrency-mining-why-use-fpga-for-mining-fpga-vs-gpu-vs-asic-explained-5aaa400082b9.
50. Arrow. *FPGA Mining: What is FPGA Mining in Cryptocurrency?* [Online] Arrow, 27. Září 2018. [Citace: 8. Únor 2023.] https://www.arrow.com/en/research-and-events/articles/silicon-labs-ble-matter-workshops.
51. Frankenfield, Jake. Investopedia. *Mining Pool: Definition, How It Works, Methods, and Benefits.* [Online] Investopedia, 15. Leden 2022. [Citace: 15. Únor 2023.] https://www.investopedia.com/terms/m/mining-pool.asp.
52. Merchant, Murtuza. CoinTelegraph. *What is a cryptocurrency mining pool?* [Online] CoinTelegraph, 24. Září 2022. [Citace: 15. Únor 2023.] https://cointelegraph.com/news/what-is-a-cryptocurrency-mining-pool.
53. bitcoin.it. *Comparison of mining pools.* [Online] 18. Březen 2022. [Citace: 15. Únor 2023.] https://en.bitcoin.it/wiki/Comparison_of_mining_pools.
54. BlockChain. *Bitcoin Block 777,162.* [Online] BlockChain, 16. Únor 2023. [Citace: 16. Únor 2023.] https://www.blockchain.com/explorer/blocks/btc/777162.
55. minebest. *Different mining pool payouts explained: PPS vs. FPPS vs. PPLNS vs. PPS+.* [Online] 6. Září 2021. [Citace: 16. Únor 2023.] https://minebest.com/blog/pps-vs-fpps-vs-pplns-vs-pps-mining-pool-payouts-explained.
56. Burritos, Side Of. YouTube. *Mining Pools Explained - PPLNS vs PPS | Payout Methods.* [Online] YouTube - Side of Burritos, 1. Červen 2021. [Citace: 16. Únor 2023.] https://www.youtube.com/watch?v=6WcV4nS4ti0&ab_channel=SideOfBurritos.
57. console.cudominer.com. *CudoMiner Dashboard.* [Online] Cudo. [Citace: 26. Únor 2023.] Únor. https://console.cudominer.com/dashboard/.
58. Elektřina - ceny a grafy elektřiny, vývoj ceny elektřiny 1 kWh - 16 let - měna CZK. *Kurzy.cz.* [Online] Kurzy, 23. Únor 2023. [Citace: 26. Únor 2023.] https://www.kurzy.cz/komodity/cena-elektriny-graf-vyvoje-ceny/1kWh-czk-30-let.
59. Bitcoin greenhouse gas emissions. *Cambridge Centre for Alternative Finances.* [Online] Univesrity of Cambridge, 27. Únor 2023. [Citace: 27. Únor 2023.] https://ccaf.io/cbeci/ghg/index.
60. Bitcoin greenhouse gas emissions: Methodology. *Cambridge Centre for Alternative Finances.* [Online] University of Cambridge. [Citace: 27. Únor 2023.] https://ccaf.io/cbeci/ghg/methodology.

61. Per capita CO_2 emissions: Czechia, Switzerland. *Our World in Data.* [Online] University of Oxford. [Citace: 27. Únor 2023.] https://ourworldindata.org/grapher/co-emissions-per-capita?tab=chart&time=2012..latest&country=CZE~CHE.
62. Population change - year 2021 - Table 1. *Czech Statistical Office.* [Online] czso - csu, 21. Březen 2022. [Citace: 21. Únor 2023.] https://www.czso.cz/csu/czso/ari/population-change-year-2021.
63. Switzerland overview - The world bank . *The world bank data.* [Online] [Citace: 27. Únor 2023.] https://data.worldbank.org/indicator/SP.POP.TOTL?locations=CH.
64. Cambridge Bitcoin Electricity Consumption Index: Bitcoin network power demand. *Cambridge Centre for Alternative Finances.* [Online] University of Cambridge, 27. Únor 2023. [Citace: 27. Únor 2023.] https://ccaf.io/cbeci/index.
65. ČTVRTLETNÍ ZPRÁVA O PROVOZU ELEKTRIZAČNÍ SOUSTAVY ČR ZA I. ČTVRTLETÍ 2022. *Energetický regulační úřad.* [Online] 18. Říjen 2022. [Citace: 27. Únor 2023.] https://www.eru.cz/ctvrtletni-zprava-o-provozu-elektrizacni-soustavy-cr-za-i-ctvrtleti-2022.
66. ČTVRTLETNÍ ZPRÁVA O PROVOZU ELEKTRIZAČNÍ SOUSTAVY ČR ZA II. ČTVRTLETÍ 2022. *Energetický regulační úřad.* [Online] 18. Říjen 2022. [Citace: 27. Únor 2023.] https://www.eru.cz/ctvrtletni-zprava-o-provozu-elektrizacni-soustavy-cr-za-ii-ctvrtleti-2022.
67. ČTVRTLETNÍ ZPRÁVA O PROVOZU ELEKTRIZAČNÍ SOUSTAVY ČR ZA III. ČTVRTLETÍ 2022. *Energetický regulační úřad.* [Online] 16. Listopad 2022. [Citace: 27. Únor 2023.] https://www.eru.cz/ctvrtletni-zprava-o-provozu-elektrizacni-soustavy-cr-za-iii-ctvrtleti-2022.
68. ČTVRTLETNÍ ZPRÁVA O PROVOZU ELEKTRIZAČNÍ SOUSTAVY ČR ZA IV. ČTVRTLETÍ 2022. *Energetický regulační úřad.* [Online] 16. Únor 2023. [Citace: 27. Únor 2023.] https://www.eru.cz/ctvrtletni-zprava-o-provozu-elektrizacni-soustavy-cr-za-iv-ctvrtleti-2022.
69. Electricity consumption by Country 2023. *World Population Review.* [Online] [Citace: 27. Únor 2023.] https://worldpopulationreview.com/country-rankings/electricity-consumption-by-country.